10

THE QUARTERLY JOURNAL OF

MATHEMATICS

OXFORD SECOND SERIES

Volume 4 *No.* 13 *March* 1953

P. D. Watson: On the Limits of Sequences of Sets . . 1

L. Carlitz: Distribution of Primitive Roots in a Finite Field 4

M. E. Noble: Non-measurable Interpolation Sets (III). A Theorem of B. J. Maitland 11

F. W. Ponting: The Location of Singularities on the Circle of Convergence of Gap Series (I) 19

E. J. Scott: Jacobi Transforms 36

J. G. Brennan: Manifolds whose Points image Pairs or Trios of Points chosen from the Groups of a Linear Series 41

A. Oppenheim: Values of Quadratic Forms (I) . . 54

A. Oppenheim: Values of Quadratic Forms (II) . . 60

D. G. Northcott: Hilbert's Function in a Local Ring . 67

THE JOHN CRERAR
APR 27 1953
LIBRARY

OXFORD
AT THE CLARENDON PRESS

Price 12*s.* 6*d. net*

PRINTED IN GREAT BRITAIN BY CHARLES BATEY AT THE UNIVERSITY PRESS, OXFORD

THE QUARTERLY JOURNAL OF
MATHEMATICS

OXFORD SECOND SERIES

Edited by T. W. CHAUNDY, U. S. HASLAM-JONES,
J. H. C. THOMPSON

THE QUARTERLY JOURNAL OF MATHEMATICS (OXFORD SECOND SERIES) is published at 12s. 6d. net for a single number with an annual subscription (for four numbers) of 44s. 6d. post free.

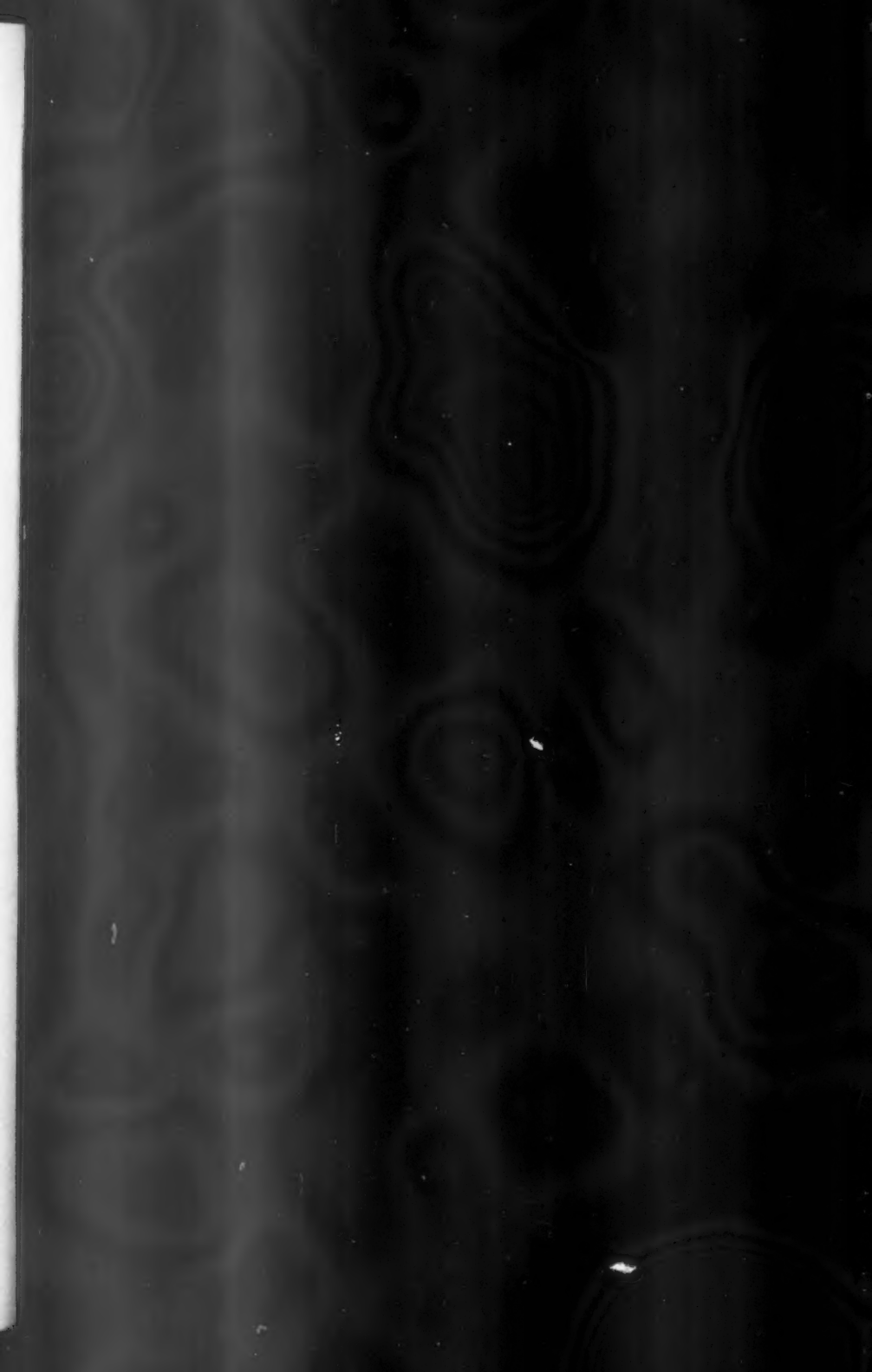
Papers, of a length normally not exceeding 20 printed pages of the Journal, are invited on subjects of Pure and Applied Mathematics, and should be addressed 'The Editors, Quarterly Journal of Mathematics, Clarendon Press, Oxford'. They should be in a condition fit for sending to a referee and in form and notation convenient for printing. The Editors as a rule will not wish to accept material that they cannot see their way to publish within a twelvemonth.

While every care is taken of manuscripts submitted for publication, the Publisher and the Editors cannot hold themselves responsible for any loss or damage. Authors are advised to retain a copy of anything they may send for publication. Authors of papers printed in the Quarterly Journal will be entitled to 50 free offprints.

Correspondence on the *subject-matter* of the Quarterly Journal should be addressed, as above, to 'The Editors', at the Clarendon Press. All other correspondence should be addressed to the Publisher:—

GEOFFREY CUMBERLEGE
OXFORD UNIVERSITY PRESS
AMEN HOUSE, LONDON, E.C.4

The publishers are signatories to the Fair Copying Declaration in respect of this journal. Details of the Declaration may be obtained from the offices of the Royal Society upon application.



ON THE LIMITS OF SEQUENCES OF SETS

By P. D. WATSON (*Oxford*)

[Received 12 September 1950]

It has been shown by Kuratowski† that, if $\mathbf{X}$ is a separable metric space, then the set of closed subsets of $\mathbf{X}$ is an L^*-space $(2^{\mathbf{X}})_L$ which is separable and countably compact, the limit of a sequence of sets being taken in the sense of Hausdorff.‡ In the case where $\mathbf{X}$ is a compact metric space it is known§ that $(2^{\mathbf{X}})_L$ is a compact metric space, but Kuratowski‖ has given an example of non-compact space $\mathbf{X}$ such that $(2^{\mathbf{X}})_L$ is not even a topological space. The theorem which follows relates the topological structure of $(2^{\mathbf{X}})_L$ to that of $\mathbf{X}$.

THEOREM. *If* $\mathbf{X}$ *is a separable metric space, then*

(i) *if* $\mathbf{X}$ *is not locally compact, then* $(2^{\mathbf{X}})_L$ *is not a topological space;*

(ii) *if* $\mathbf{X}$ *is locally compact, then* $(2^{\mathbf{X}})_L$ *is a compact metric space.*

Proof. (i) Suppose that $\mathbf{X}$ is not locally compact.

Since $\mathbf{X}$ is a separable metric space, it can, by Urysohn's theorem, be topologically embedded in a compact metric space $\mathbf{X}^*$; we can, moreover, assume that $\mathbf{X}$ is dense in $\mathbf{X}^*$, otherwise replacing $\mathbf{X}^*$ by the closure of $\mathbf{X}$ in $\mathbf{X}^*$. We shall find it necessary to distinguish between the limits of sequences of points and sequences of sets in $\mathbf{X}$ and in $\mathbf{X}^*$: limits in $\mathbf{X}$ will be denoted as usual by 'lim', while limits in $\mathbf{X}^*$ will be denoted by 'Lim'. Thus, if $\{x_n\}$ is a sequence of elements of $\mathbf{X}$, $\operatorname{Lim} x_n$ may exist although $\lim x_n$ does not, but, if $\operatorname{Lim} x_n$ exists and belongs to $\mathbf{X}$, then $\lim x_n = \operatorname{Lim} x_n$. Similarly, if $\{E_n\}$ is a sequence of subsets of $\mathbf{X}$, $\lim E_n$ may exist although $\operatorname{Lim} E_n$ does not, but, if $\operatorname{Lim} E_n$ exists, then

$$\lim E_n = \mathbf{X} \cap \operatorname{Lim} E_n.$$

I shall denote the metric in $\mathbf{X}$ by ρ. If a is a point of $\mathbf{X}$ and $\delta > 0$, I shall write

$$V(\delta; a) = E[x \in \mathbf{X}^*, \rho(a, x) < \delta].$$

Let $\mathbf{CX}$ be the complement of $\mathbf{X}$ considered as a subset of $\mathbf{X}^*$. Then $\mathbf{CX}$ is not closed; for otherwise $\mathbf{X}$ would be an open subset of a compact space, and consequently itself locally compact, contrary to hypothesis. It follows that there is a point a_ω of $\mathbf{X}$ which is a limit point of $\mathbf{CX}$, and hence that there exists a sequence $\{a_n\}$ $(n = 1, 2, \ldots)$ of distinct

† Kuratowski (**3**) 157.

‡ Hausdorff (**2**) 146–7.

§ Hausdorff (**2**) 148–50.

‖ Kuratowski (**3**) 157.

points of $\mathbf{CX}$ such that $\operatorname{Lim} a_n = a_\omega$. Further, since the points of $\{a_n\}$ are distinct, we can find a sequence $\{\delta_n\}$ of positive numbers such that $\lim \delta_n = 0$ and such that the sets $V(\delta_n; a_n)$ are mutually exclusive and a_ω is a point of none of them. It now follows from the fact that $\mathbf{X}$ is dense in $\mathbf{X}^*$ that we can find for every positive integer n a sequence $\{b_{nm}\}$ $(m = 1, 2, \ldots)$ of distinct points such that

$$b_{nm} \in X \cap V(\delta_n; a_n) \quad \text{and} \quad \operatorname*{Lim}_{m\to\infty} b_{nm} = a_n.$$

The elements of the double sequence $\{b_{nm}\}$ are all distinct because the sets $V(\delta_n; a_n)$ are mutually exclusive: let them be rearranged as a simple sequence $\{c_p\}$ $(p = 0, 1, 2, \ldots)$. We now define $\mathscr{E}$ to be the subset $\bigcup_{m,n=1}^{\infty} (E_{mn})$ of $(2X)_L$, where $E_{mn} = (c_0) \cup (c_n) \cup (b_{nm})$. If $(2X)_L$ were a topological space, we should have $\overline{\overline{\mathscr{E}}} = \overline{\mathscr{E}}$. Hence in order to prove the first half of the theorem it suffices to show that $\overline{\overline{\mathscr{E}}} \neq \overline{\mathscr{E}}$; we shall, in fact, show that

$$(c_0) \in \overline{\overline{\mathscr{E}}} \cap \mathbf{C}\overline{\mathscr{E}}.$$

Let $\{S_i\}$ be any convergent sequence of elements of $\mathscr{E}$, and suppose that $S_i = E_{m_i n_i}$. The sequence $\{n_i\}$ may or may not contain an infinite number of different integers; we shall consider the two cases separately.

First suppose that there are an infinite number of different integers n_i. We can without loss suppose further that the sequence $\{n_i\}$ is monotonic increasing, otherwise replacing $\{S_i\}$ by a suitably chosen subsequence. Hence, since

$$\begin{aligned} \rho\{a_\omega, b_{n_i m_i}\} &\leqslant \rho\{a_\omega, a_{n_i}\} + \rho\{a_{n_i}, b_{m_i n_i}\} \\ &\leqslant \rho\{a_\omega, a_{n_i}\} + \delta_{n_i}, \end{aligned}$$

it follows that

$$\lim_{i\to\infty} \rho\{a_\omega, b_{n_i m_i}\} = 0.$$

We conclude that $a_\omega \in \lim S_i$.

Secondly, suppose that there are only a finite number of different integers n_i. In this case we may suppose that *all* the n_i are the same integer, p say, otherwise replacing $\{S_i\}$ by a suitably chosen subsequence. It follows that $c_p \in S_i$ for every i, and hence that $c_p \in \lim S_i$.

We have thus shown that every set which is the limit of a sequence of elements of $\mathscr{E}$, i.e. every element of $\overline{\mathscr{E}}$, contains at least one of the points $a_\omega, c_1, c_2, \ldots$. Hence the single-point set (c_0) is not an element of $\overline{\mathscr{E}}$. On the other hand it is evident that

$$\operatorname*{Lim}_{m\to\infty} E_{mp} = (c_0) \cup (c_p) \cup (a_p),$$

and hence that

$$\lim_{m\to\infty} E_{mp} = (c_0) \cup (c_p).$$

Consequently $(c_0) \cup (c_p) \in \overline{\overline{\mathscr{E}}} \quad (p = 1, 2,...).$

Now, since $\{c_p\}$ is a rearrangement of the double sequence $\{b_{nm}\}$, there is a sequence $\{p_j\}$ such that $\{c_{p_j}\}$ $(j = 1, 2,...)$ is a rearrangement of $\{b_{1m}\}$ $(m = 1, 2,...)$. It follows that

$$\operatorname*{Lim}_{j\to\infty}\{(c_0) \cup (c_{p_j})\} = (c_0) \cup (a_1),$$

and hence that $$\lim_{j\to\infty}\{(c_0) \cup (c_{p_j})\} = (c_0).$$

We have thus shown that $(c_0) \in \overline{\overline{\mathscr{E}}}$, and this completes the proof of the first part of the theorem.

(ii) Suppose now that $\mathbf{X}$ is locally compact; we assume that $\mathbf{X}$ is not compact, since otherwise we are in the case of Hausdorff mentioned above. By Alexandroff's theorem,† we can embed $\mathbf{X}$ in a compact metric space $\mathbf{X}^*$ by the addition of a single point ω. By associating the closed subset F of $\mathbf{X}$ with the closed subset $F \cup (\omega)$ of $\mathbf{X}^*$ we set up a one-to-one correspondence between $(2^{\mathbf{X}})_L$ and a subset of the compact metric space $(2^{\mathbf{X}^*})_L$ which is itself closed and therefore a compact metric space. This correspondence is evidently a homeomorphism, and we conclude that $(2^{\mathbf{X}})_L$ is a compact metric space. This completes the proof of the theorem.

† Alexandroff (**1**).

REFERENCES

1. Alexandroff, 'Über die Metrisation der im kleinen kompakten topologischen Raume', *Math. Ann.* 92 (1924), 299.
2. Hausdorff, *Mengenlehre* (Berlin, 1927).
3. Kuratowski, *Topologie* (*I*) (Warsaw, 1933).

DISTRIBUTION OF PRIMITIVE ROOTS IN A FINITE FIELD

By L. CARLITZ (*Duke University*)

[Received 27 December 1951]

1. Introduction

DAVENPORT (**2**) has proved that, if the prime p is sufficiently large and θ is a generating element of the finite field $GF(p^n)$, then there exists an integer $a \pmod p$ such that $\theta+a$ is a primitive root of the field. On the other hand, he proved that for given p there exist fields $GF(p^n)$ and generating elements θ such that no number of the form $a\theta+b$ is a primitive root.

In the present note I shall extend Davenport's results in several directions. Let $e|(p^n-1)$ and let θ have the same meaning as above; then using Davenport's principal lemma I show that the number of numbers in $GF(p^n)$ of the form $\theta+a$ belonging to the exponent e is

$$\frac{\phi(e)}{p^n-1}p+O(p^{1-\{1/2(n+1)\}+\epsilon}). \tag{1.1}$$

More generally, if $N_r(e)$ denotes the number of numbers

$$\theta^r+a_1\theta^{r-1}+\ldots+a_r \quad (a_i \in GF(p))$$

that belong to the exponent e, then using a theorem of A. Weil's (**5**), we have

$$N_r(e) = \frac{\phi(e)}{p^n-1}p^r+O(p^{\frac{1}{2}r+\epsilon}). \tag{1.2}$$

Presumably (1.2)—possibly with a poorer error term—can be proved without Weil's theorem.

In (1.1) and (1.2) it is assumed that $p \to \infty$. The following result, however, holds for all p:

$$N_r(e) = \frac{\phi(e)}{p^n-1}p^r+O(p^{\frac{1}{2}n+\epsilon}) \quad (p^n \to \infty); \tag{1.3}$$

of course (1.3) is of interest only if $r > \frac{1}{2}n$. For a more general result see Theorem 3 below.

In the next place I show that for fixed p^n, r there exist infinitely many irreducible polynomials P in $GF[p^n, x]$ such that

$$A^{(p^{nm}-1)/(p^n-1)} \equiv 1 \pmod P \quad (m = \deg P), \tag{1.4}$$

for all polynomials $A \neq 0$ of degree less than r. In particular (1.4) shows that no such A is a primitive root (mod P).

Finally we note that, if $e|(p-1)$, $s \geqslant 0$, $r \geqslant 1$, then the number of integers t $(s < t \leqslant s+r)$ which belong to the exponent $e \pmod p$ is

$$\frac{\phi(e)}{p-1}r+O(p^{\frac{1}{2}+\epsilon}). \tag{1.5}$$

The method of proof, except for (1.4), is a modification of Vinogradoff's device [(3) 178].

2. Let $ef = p^n-1$ and let $\chi(\alpha)$ denote a multiplicative character of $GF(p^n)$. Consider the function

$$\omega(\alpha) = \frac{1}{f}\sum_{d|e}\frac{\mu(d)}{d}\sum_{\chi^{df}=\chi_0}\chi(\alpha) \quad (\alpha \in GF(p^n)), \tag{2.1}$$

where the inner sum is over the df characters such that $\chi^{df} = \chi_0$, the principal character. It is easily verified that

$$\frac{1}{r}\sum_{\chi^r=\chi_0}\chi(\alpha) = \begin{cases}1 & (\alpha^s = 1),\\ 0 & (\alpha^s \neq 1),\end{cases}$$

where $rs = p^n-1$. Thus it follows that, if $d|e$,

$$\frac{1}{df}\sum_{\chi^{df}=\chi_0}\chi(\alpha) = \begin{cases}1 & (\alpha^{e|d} = 1),\\ 0 & (\alpha^{e|d} \neq 1).\end{cases}$$

If therefore $\alpha^e \neq 1$, it is clear from (2.1) that $\omega(\alpha) = 0$; if $\alpha^e = 1$, let α belong to the exponent e/t, then (2.1) implies

$$\omega(\alpha) = \sum_{d|t}\mu(d) = \begin{cases}1 & (t = 1),\\ 0 & (t \neq 1).\end{cases}$$

This proves

LEMMA 1. *If α belongs to the exponent e, then $\omega(\alpha) = 1$; otherwise $\omega(\alpha) = 0$.*

Note that when $e = p^n-1$, (2.1) does not reduce to the formula of Vinogradoff; however it is not difficult to show that the two are equivalent in this case.

We shall also require (**2**) Lemma 2.

LEMMA 2. *Let θ generate the $GF(p^n)$: that is, θ satisfies $f(\theta) = 0$, where $f(x)$ is of degree n and irreducible in $GF[p,x]$. Then, for $\chi \neq \chi_0$,*

$$\sum_{a=0}^{p-1}\chi(\theta+a) = O(p^{1-\{1/2(n+1)\}}) \quad (p \to \infty). \tag{2.2}$$

Let $N(e)$ be the number of numbers of the form $\theta+a$ that belong to the exponent e. Then by Lemma 1 it is evident that

$$N(e) = \sum_{a=0}^{p-1}\omega(\theta+a).$$

Substituting from (2.1) and separating the terms involving the principal character, we get

$$N(e) = \frac{\phi(e)}{p^n-1}p + \frac{1}{f}\sum_{d|e}\frac{\mu(d)}{d}\sum_{\substack{\chi^d=\chi_0\\ \chi\neq\chi_0}}\sum_{a=0}^{p-1}\chi(\theta+a). \tag{2.3}$$

Now using (2.2), the triple sum in the right-hand member is evidently

$$O\Big(\sum_{d|e}\mu^2(d)p^{1-\{1/2(n+1)\}}\Big) = O(p^{1-\{1/2(n+1)\}+\epsilon}),$$

since

$$\sum_{d|m}\mu^2(d) = O(m^\epsilon).$$

We thus get

THEOREM 1. *Let $N(e)$ denote the number of numbers $\theta+a$ that belong to the exponent e. Then*

$$N(e) = \frac{\phi(e)}{p^n-1}p + O(p^{1-\{1/2(n+1)\}+\epsilon}). \tag{2.4}$$

In view of the well-known estimate

$$\frac{m}{\phi(m)} = O(m^\epsilon),$$

it follows from (2.4) that, if

$$e \geqslant p^c, \qquad c > n - \frac{1}{2(n+1)}, \tag{2.5}$$

then $N(e) > 0$ for $p > p_0$. More precisely, if (2.5) holds, we have

$$N(e) \sim \frac{\phi(e)}{p^n-1}p \quad (p\to\infty).$$

On the other hand, if

$$e = O(p^{n-\{1/2(n+1)\}+\epsilon}),$$

then (2.4) implies $\qquad N(e) = O(p^{1-\{1/2(n+1)\}+\epsilon}).$

3. For $r \geqslant 1$ let $N_r(e)$ denote the number of numbers

$$\alpha = \theta^r + a_1\theta^{r-1} + \ldots + a_r \quad (a_i \in GF(p)) \tag{3.1}$$

that belong to the exponent e; thus $N_1(e) = N(e)$. Then exactly as above

$$N_r(e) = \frac{\phi(e)}{p^n-1}p^r + \frac{1}{f}\sum_{d|e}\frac{\mu(d)}{d}\sum_{\substack{\chi^d=\chi_0\\ \chi\neq\chi_0}}\sum_{\alpha}\chi(\alpha). \tag{3.2}$$

Thus we need an estimate for

$$\beta_r = \beta_r(\chi) = \sum_{\alpha}\chi(\alpha) \quad (\chi\neq\chi_0),$$

where α runs through the p^r numbers (3.1). The best such estimate is presumably obtained by introducing the function

$$L(s,\chi) = \sum_{r=0}^{n-1} \beta_r p^{-rs}, \tag{3.3}$$

for which we have the factorization

$$L(s,\chi) = \prod_{j=1}^{n-1} (1-\gamma_j p^{-s}). \tag{3.4}$$

Now let $GF(p^n)$ be defined by means of $f(\theta) = 0$, where $f(x)$ is an irreducible polynomial $\in GF[p,x]$. Construct the field

$$K = GF(p^n, x, y) \quad (y^{p^n-1} = f(x));$$

then it is easily seen that $L(x)$ divides the zeta function for K. Consequently, by Weil's theorem (**5**), we have

$$|\gamma_j| = p^{\frac{1}{2}}. \tag{3.5}$$

Hence using (3.3), (3.4), (3.5) we get

$$|\beta_r| \leqslant \binom{n-1}{r} p^{\frac{1}{2}r}. \tag{3.6}$$

Returning to (3.2), we may state

THEOREM 2. *For* $1 \leqslant r < n$,

$$N_r(e) = \frac{\phi(e)}{p^n-1} p^r + O(p^{\frac{1}{2}r+\epsilon}). \tag{3.7}$$

In particular, if $\quad e \geqslant p^{c'} \qquad (c' > n-\frac{1}{2}r), \tag{3.8}$

then $N_r(e) > 0$ for $p > p_0$. More precisely, if (3.8) holds, we have

$$N_r(e) \sim \frac{\phi(e)}{p^n-1} p^r \quad (p \to \infty).$$

On the other hand, if $e = O(p^{n-\frac{1}{2}r+\epsilon})$, then

$$N_r(e) = O(p^{\frac{1}{2}r+\epsilon}).$$

4. We have assumed that n and r are fixed as $p \to \infty$. Now as a matter of fact, it follows from (3.2) and (3.6) that

$$N_r(e) = \frac{\phi(e)}{p^n-1} p^r + O\left\{\binom{n-1}{r} p^{\frac{1}{2}r} e^{\epsilon}\right\},$$

where now the constant in O is absolute. However for $r > \frac{1}{2}n$ it is better to proceed differently. We use the familiar

$$\tau = \tau(\chi) = \sum_{\beta \in GF(p^n)} \chi(\beta) \zeta^{t(\beta)},$$

where $t(\beta) = \beta + \beta^p + \ldots + \beta^{p^{n-1}}$ and $\zeta = e^{2\pi i/p}$. Then $|\tau| = p^{\frac{1}{2}n}$ for $\chi \neq \chi_0$.

Now let $\alpha_1,\dots,\alpha_r$ be numbers of $GF(p^n)$ that are linearly independent relative to $GF(p)$, α_0 fixed; let α run through the p^r numbers

$$\alpha = \alpha_0+c_1\alpha_1+\dots+c_r\alpha_r \quad (c_i \in GF(p)). \tag{4.1}$$

Then we have $$\tau(\bar{\chi})\sum_{\alpha}\chi(\alpha) = \sum_{\beta\in GF(p^n)}\bar{\chi}(\beta)\sum_{\alpha}\zeta^{t(\alpha\beta)},$$

and we can show without much trouble that, for $\chi \neq \chi_0$, the inner sum in the right-hand member vanishes except for p^{n-r} values of β, namely those for which $t(\alpha\beta) = 0$. It follows that

$$\Big|\sum_{\alpha}\chi(\alpha)\Big| \leqslant p^{\frac{1}{2}n}.$$

If $N_r^*(e)$ denotes the number of numbers (4.1) that belong to the exponent e, then as above we find

$$N_r^*(e) = \frac{\phi(e)}{p^n-1}p^r+O\Big(p^{\frac{1}{2}n}\sum_{d|e}\mu^2(d)\Big), \tag{4.2}$$

where the constant in O is absolute. This proves

THEOREM 3. *For all p and when $1 \leqslant r \leqslant n$, (4.2) holds. In particular, if $r > \frac{1}{2}n$ and $e \geqslant p^c$, where $c > \frac{3}{2}n-r$, then*

$$N_r^*(e) \sim \frac{\phi(e)}{p^n-1}p^r \quad (p^n \to \infty).$$

Evidently (1.3) is contained in Theorem 3.

5. I now prove the following extension of (**1**) Theorem 2.

THEOREM 4. *For fixed p^n, $r \geqslant 1$, there exist infinitely many irreducible polynomials $P(x) \in GF[p^n, x]$ such that*

$$A^{(p^{nm}-1)/(p^n-1)} \equiv 1 \pmod{P} \quad (m = \deg P), \tag{5.1}$$

for all polynomials $A \neq 0$ of degree $< r$.

Clearly (5.1) implies in particular that no such A is a primitive root (mod P).

The proof of Theorem 4 depends on the existence of infinitely many irreducibles P such that $(p^n-1)|\deg P$ and

$$P \equiv 1 \pmod{L_r}, \tag{5.2}$$

where L_r is the least common multiple of the A's. (It can be proved that

$$L_r = (x^{p^{nr}}-x)(x^{p^{n(r-1)}}-x)\dots(x^{p^n}-x);$$

however, the exact form of L_r will not be needed.) The existence of irreducibles P satisfying the conditions stated is of course a consequence of Artin's refinement [(**1**) 246] of Kornblum's theorem.

It is clear that, if A and B satisfy (5.1), then the same is true of AB.

Thus it is only necessary to verify that (5.1) holds for $A = \alpha Q$, where $\alpha \in GF(p^n)$ and Q is irreducible in $GF[p^n, x]$ of degree less than r. Now in the first place, if $\alpha \neq 0$, it follows from $(p^n-1)|m$ that

$$\alpha^{(p^{nm}-1)/(p^n-1)} = 1,$$

so we need consider only $A = Q$. While we can dispose of this case by using the reciprocity theorem, it is perhaps better to give a direct proof [compare (4)]. Let $\deg Q = k$ and put

$$P(x) = \prod_{i=0}^{m-1} (x-\pi^{p^{ni}}), \qquad Q(x) = \prod_{i=0}^{k-1} (x-\rho^{p^{ni}}),$$

where $\pi \in GF(p^{nm})$, $\rho \in GF(p^{nk})$. Now (5.2) implies $P \equiv 1 \pmod{Q}$ and therefore

$$\prod_{i=0}^{m-1} (\rho-\pi^{p^{ni}}) \equiv 1 \pmod{(x-\rho)}.$$

Consequently

$$\prod_{i=0}^{m-1} \prod_{j=0}^{k-1} (\rho^{p^{nj}}-\pi^{p^{ni}}) = 1. \tag{5.3}$$

On the other hand

$$Q^{(p^{nm}-1)/(p^n-1)} \equiv \prod_{j=0}^{k-1} (\pi-\rho^{p^{nj}})^{1+p^n+\cdots+p^{n(m-1)}}$$

$$\equiv \prod_{i=0}^{m-1} \prod_{j=0}^{k-1} (\pi^{p^{ni}}-\rho^{p^{nj}}) \pmod{(x-\pi)}.$$

Since $(p^n-1)|m$, it follows from (5.3) that

$$Q^{(p^{nm}-1)/(p^n-1)} \equiv 1 \pmod{P}.$$

This completes the proof of the theorem.

6. Suppose now that $e|(p-1)$, $r \geqslant 1$, $s \geqslant 0$. Let $N(e,r) = N(e,r,s)$ denote the number of integers t $(s < t \leqslant s+r)$ which belong to the exponent e. If, in § 2, we take $n = 1$, $ef = p-1$, then it is clear that

$$N(e,r) = \sum_{m=s+1}^{s+r} \omega(m),$$

where $\omega(m)$ is defined exactly as before. Thus, by (2.1),

$$N(e,r) = \frac{\phi(e)}{p-1} r + \frac{1}{f} \sum_{d|e} \frac{\mu(d)}{d} \sum_{\substack{\chi^{df}=\chi_0 \\ \chi \neq \chi_0}} \sum_{m=s+1}^{s+r} \chi(m).$$

Now, by (3) Theorem 494, for $\chi \neq \chi_0$,

$$\left| \sum_{m=s+1}^{s+r} \chi(m) \right| < p^{\frac{1}{2}} \log p.$$

Completing the argument in the usual way, we get

THEOREM 5. *For $N(e,r)$ as defined above,*

$$N(e,r) = \frac{\phi(e)}{p-1}r + O\Big(p^{\frac{1}{2}}\log p \sum_{d|e}\mu^2(d)\Big)$$

$$= \frac{\phi(e)}{p-1}r + O(p^{\frac{1}{2}+\epsilon}).$$

In particular, if $er \geqslant p^c$, $c > \frac{3}{2}$, then

$$N(e,r) \sim \frac{\phi(e)}{p-1}r \quad (p \to \infty).$$

REFERENCES

1. E. Artin, 'Quadratische Körper im Gebiete der höheren Kongruenzen', *Math. Zeits.* 19 (1924), 207–46.
2. H. Davenport, 'On primitive roots in finite fields', *Quart. J. of Math.* (Oxford), 8 (1937), 308–12.
3. E. Landau, *Vorlesungen über Zahlentheorie* (Leipzig 1927), vol. 2.
4. F. K. Schmidt, 'Zur Zahlentheorie in Körpern von der Characteristik p', *Erlanger Sitz.* 58–59 (1928), 159–72.
5. A. Weil, 'On the Riemann hypothesis in function fields', *Proc. National Acad. of Sci.* 27 (1941), 345–7.

NON-MEASURABLE INTERPOLATION SETS (III) A THEOREM OF B. J. MAITLAND

By M. E. NOBLE (*Nottingham*)

[Received 9 January 1951]

1. B. J. MAITLAND (**1**) has proved

THEOREM A. *If $f(z)$ is an integral function of finite order ρ and mean type κ and $d < (\pi/2\kappa\rho^2)^{\frac{1}{2}}$, there exists a sequence ζ_n such that $|\zeta_n| \to \infty$ as $n \to \infty$, and*

$$\lim |z|^{-\rho} \log|f(z)| = \kappa$$

as $|z| \to \infty$ in the circles $|z-\zeta_n| \leqslant d|\zeta_n|^{1-\frac{1}{2}\rho}$.

By methods similar to those used in the present author's previous papers on non-measurable interpolation sets [Noble (**2**), (**3**), particularly (**2**)], we are able to refine Theorem A so as to obtain

THEOREM B. *Suppose that $f(z)$ is an integral function of finite order $\rho > 1$ and mean type κ, that $\mu < \kappa$, $d < (\pi/2\kappa\rho^2)^{\frac{1}{2}}$ and that $E(f, \kappa, \mu, d)$ is the set of r such that, for some $\zeta(r)$ with $|\zeta(r)| = r$,*

$$\log|f(z)| \geqslant \mu r^\rho$$

when $|z-\zeta(r)| \leqslant dr^{1-\frac{1}{2}\rho}$. Then for some $C(\rho) \geqslant \dfrac{e(\rho-1)}{\rho^2}$

$$\limsup_{R\to\infty} \frac{\text{meas } E \cap [0, R]}{R} = D^*E \geqslant C(\rho)\left(1-\frac{2\rho^2d^2\kappa}{\pi}\right)\min\left\{\frac{1}{2}\left(1-\frac{2\rho^2d^2\kappa}{\pi}\right), 1-\frac{\mu}{\kappa}\right\}. \quad (1.1)$$

If $0 < \rho \leqslant 1$, we obtain less accessible results in terms of the function $\tau_\rho(\theta)$ [cf. (**2**) § 2] defined by

$$\tau_\rho(\theta) = \sup_{\text{meas } E \leqslant \theta} \rho^2 \int_E x^{\rho-1} \log\frac{1}{x}\, dx. \quad (1.2)$$

THEOREM C. *Suppose that $f(z)$ is an integral function of finite order ρ and mean type κ, that $\mu < \kappa$, $d < (\pi/2\kappa\rho^2)^{\frac{1}{2}}$ and that $E(f, \kappa, \mu, d)$ is the set of r such that, for some $\zeta(r)$ with $|\zeta(r)| = r$,*

$$\log|f(z)| \geqslant \mu r^\rho$$

when $|z-\zeta(r)| \leqslant dr^{1-\frac{1}{2}\rho}$. Then, if $\lambda_0 > 0$ is defined by

$$1-\frac{2\rho^2(1+\lambda_0)^2d^2\kappa}{\pi} = \frac{1}{2}\left(1-\frac{2\rho^2d^2\kappa}{\pi}\right) \quad (1.3)$$

and $\Lambda = D^*E$,

$$\tau_\rho\left(\frac{\Lambda(1+\lambda_0)}{\lambda_0}\right) \geqslant \min\left\{\frac{1}{2}\left(1-\frac{2\rho^2 d^2\kappa}{\pi}\right),\ 1-\frac{\mu}{\kappa}\right\}. \tag{1.4}$$

These results could certainly be improved by further elementary manipulation or by a more sophisticated choice of λ_0, but, since the method cannot yield a best-possible result, we confine ourselves to the above results which illustrate the method and probably show the correct form of dependence on $\kappa-\mu$ and $1-2\rho^2 d^2\kappa/\pi$.

2. It is convenient to use a dissection of the complex plane introduced by G. Valiron [(**4**) 74]. I shall mean by *the Valiron dissection of mesh* δ the set of regions ('quadrilaterals') $Q_{s,t}$ $(s, t = 1, 2,\ldots)$ defined by

$$r_s \leqslant |z| < r_{s+1},$$

$$t\,\delta'(s) \leqslant \arg z < (t+1)\,\delta'(s),$$

where $r_1 = 1$, and $r_{s+1}-r_s = \delta r_s^{1-\frac{1}{2}\rho}$,

$$\delta'(s) = \frac{2\pi}{1+[2\pi\delta^{-1}r_s^{\frac{1}{2}\rho}]} = \frac{2\pi}{\eta_s}.$$

Otherwise I adopt the notation of (**2**) § 2.3.

We begin by recalling some of the ideas of (**2**). A sequence $\{z_n\}$ will be said to *belong* to $\mathscr{G}(D^*, d^*, \eta, \rho)$ if there exists an integral function $\sigma_g(z)$ vanishing for all z_n and to any $\epsilon > 0$ corresponds $R_0(\epsilon)$ such that, when $R > R_0$ and $|z| \leqslant R$,

$$\log|\sigma_g(z)| \leqslant (D^*+\epsilon)r^\rho, \tag{2.1}$$

$$\log|\sigma_g(z)| \geqslant (d^*-\epsilon)r^\rho, \tag{2.2}$$

except for a set $e(R)$ of z of radial measure at most ηR; and further, when $|z_n| \geqslant R_0$,

$$\log|\sigma_g'(z_n)| \geqslant (d^*-\epsilon)|z_n|^\rho. \tag{2.3}$$

The following interpolation result is a slightly modified form of Lemma 11 of (**2**).

LEMMA 1. *Suppose that* $\{z_n\}$ *belongs to* $\mathscr{G}(D^*, d^*, \eta, \rho)$ *and that* $f(z)$ *is an integral function of type* κ *and order* ρ *such that*

$$\kappa < d^*(1+2\eta)^{-\rho}.$$

Then, if

$$\beta = \limsup|z_n|^{-\rho}\log|f(z_n)|,$$

$$\kappa \leqslant \left(\beta\frac{d^*}{D^*}+D^*-\frac{d^{*2}}{D^*}\right)(1+2\eta)^\rho. \tag{2.4}$$

The work of the present paper is based on the application of Lemma 1 to the particular sequences $\{z_n\}$ and functions $\sigma_g(z)$ defined as follows. Let $\mathscr{E}$ be a set of positive r such that $\Theta = D^*\mathscr{E} < 1$, and $Q_{s,t}$ a Valiron dissection of mesh δ. Let z_n $(n = 1, 2,...)$ be a complex sequence such that, for some $h > 0$, if $m \neq n$,

$$|z_m - z_n| \geqslant h \min(|z_n|^{1-\frac{1}{2}\rho}, |z_m|^{1-\frac{1}{2}\rho}) \tag{2.5}$$

and such that $Q_{s,t}$ contains a single z_n (denoted by $z_{s,t}$) if and only if $Q_{s,t}$ is not entirely covered by $\mathscr{E}$. We have the following lemma.

LEMMA 2. (i) *As* $u \to \infty$

$$n_1(u) = n(r_s \leqslant u) \sim \frac{2}{\rho\delta} u^{\frac{1}{2}\rho}.$$

(ii) *If* m *is an integer not less than* ρ, *there exists*

$$\alpha = \lim_{u\to\infty} \sum_{|z_{s,t}| \leqslant u} z_{s,t}^{-m}.$$

For, if $r_n < r < r_{n+1}$,

$$r_n = r_1 + \delta \int_0^r u^{1-\frac{1}{2}\rho}\, dn_1(u).$$

Integrating by parts and rearranging we have

$$\frac{2n_1(r)}{\rho r^{\frac{1}{2}\rho}} + \left(1 - \frac{2}{\rho}\right)\frac{1}{r}\int_0^r \frac{n_1(u)}{u^{\frac{1}{2}\rho}}\, du \underset{u}{\to} \frac{2}{\rho\delta}$$

and (i) follows by a theorem of Mercer [cf. Rado (**5**)].

Also $$\sum_{|z_{s,t}| \leqslant u} z_{s,t}^{-m} = \sum_{|z_{s,t}| \leqslant u} (z_{s,t}^{-m} - \zeta_{s,t}^{-m}),$$

where $\zeta_{s,t} = r_s \exp it\,\delta'(s)$. Using (i) we have

$$\left|\sum_t (z_{s,t}^{-m} - \zeta_{s,t}^{-m})\right| \leqslant K\delta^{-1} r_s^{\frac{1}{2}\rho} \frac{\delta r_s^{1-\frac{1}{2}\rho}}{r_s^{m+1}}$$

$$\leqslant \frac{K}{r_s^m} \leqslant K s^{-2m/\rho}$$

and (ii) follows since $2m/\rho \geqslant 2$.

By Lemma 2 we are justified in defining

$$\sigma_g(z, \delta, \mathscr{E}) = \sigma_\delta(z) = F(z) \prod_{z_{s,t}} E\left(\frac{z}{z_{s,t}}, p\right) \tag{2.6}$$

where $p = [\rho]$ and $F(z) = \exp\{-(\alpha/p)z^p\}$ or 1 according to whether ρ is or is not an integer. We now have

LEMMA 3. *There exist positive numbers $\kappa(\rho)$, $m(\rho)$, $\delta_0(\rho)$ such that, if $\delta < \delta_0(\rho)$, $\sigma_\delta(z)$ belongs to $\mathscr{G}(D^*, d^*, \delta, \rho)$ where*

$$D^* = \frac{2\pi}{\rho^2\delta^2}\left(1+\kappa\delta^m \log\frac{1}{\delta}\right) \quad \textit{and} \quad d^* = \frac{2\pi}{\rho^2\delta^2}\left(1-\tau_\rho(\Theta)-\kappa\delta^m\log\frac{1}{\delta}\right).$$

The proof of Lemma 3 proceeds on similar lines to that of Theorem 1 of (**2**) given in detail in (**2**) § 6.7 and we therefore abbreviate considerably.

We assume that $\delta < \frac{1}{4}$, so that $\delta^{\frac{1}{2}} < 1-\delta^{\frac{1}{2}}$ and, writing $\lambda = (1-\delta^{\frac{1}{2}})$, consider for large R the dissection of $\sigma_\delta(z)$

$$\sigma_\delta(z) = F(z)\exp\left\{\frac{z^p(p-q)}{q}\sum_{r_s\leqslant\delta^{-\frac{1}{2}}R} z_{s,t}^{-p}\right\}\prod_{r_s\leqslant\lambda R} E\left(\frac{z}{z_{s,t}},q\right)\times$$

$$\times \prod_{\lambda R<r_s\leqslant\lambda^{-1}R} E\left(\frac{z}{z_{s,t}},q\right)\prod_{\lambda^{-1}R<r_s\leqslant\delta^{-\frac{1}{2}}R} E\left(\frac{z}{z_{s,t}},q\right)\prod_{r_s>\delta^{-\frac{1}{2}}R} E\left(\frac{z}{z_{s,t}},p\right)$$

$$= \Pi_1\Pi_2\Pi_3\Pi_4\Pi_5, \quad (2.7)$$

where $$\tfrac{1}{2}(1+\lambda)R \leqslant |z| \leqslant \frac{1}{2\lambda}(1+\lambda)R.$$

By Lemma 2 we can choose $R_0(\delta)$ such that, if $R \geqslant R_0$,

$$|\log|\Pi_1(z)|| \leqslant \delta r^\rho. \quad (2.8)$$

Arguing as in Lemma 7 of (**2**) we can show that, if $R \geqslant R_1(\delta) \geqslant R_0(\delta)$,

$$|\log|\Pi_5(z)|| \leqslant K_\rho\delta^{\frac{1}{2}(p+1-\rho)}\delta^{-2}r^\rho.\dagger \quad (2.9)$$

To deal with $\Pi_4(z)$ we compare with

$$\varpi_4(z) = \prod_{\lambda^{-1}R<r_s\leqslant\delta^{-\frac{1}{2}}R} E\left(\frac{z}{\zeta_{s,t}},q\right).$$

By an argument similar to that of Lemma 9 of (**2**) we can show that

$$|\log|\Pi_4(z)|| \leqslant K_\rho\delta^{-2-\frac{1}{2}\rho}\log\frac{1}{\delta}r^{\frac{1}{2}\rho}$$

$$\leqslant \delta r^\rho \quad (2.10)$$

if $R \geqslant R_2(\delta) \geqslant R_1(\delta)$. The factor $\Pi_3(z)$ produces the exceptional set of z and we apply the lemma of H. Cartan [(**2**) Lemma 1]. If $R \geqslant R_4(\delta)$, the number of $z_{s,t}$ involved does not exceed

$$K_\rho\delta^{-1}R^{\frac{1}{2}\rho}\{n_1(\lambda^{-1}R)-n_1(\lambda R)\} \leqslant K_\rho\delta^{-2}\{\lambda^{-\frac{1}{2}\rho}-\lambda^{\frac{1}{2}\rho}\}R^\rho$$

$$\leqslant K_\rho\delta^{-\frac{1}{2}}R^\rho;$$

† K_ρ denotes a number depending only on ρ not necessarily the same at each occurrence.

and, arguing as in Lemma 8 of (**2**), we have

$$|\log|\Pi_3(z)|| \leqslant K_\rho \delta^{-\frac{1}{2}} \log\frac{1}{\delta} r^\rho \tag{2.11}$$

except for a set of z of radial measure not exceeding $\delta^{\frac{1}{2}}R$. Combining (2.8), (2.9), (2.10), and (2.11) we obtain an $R_5(\delta)K_\rho, m_1(\rho) > 0$ such that, if $R > R_5$ and $\frac{1}{2}(1+\lambda)R \leqslant |z| \leqslant \dfrac{1}{2\lambda}(1+\lambda)R$,

$$|\log|\Pi_1\Pi_3\Pi_4\Pi_5|| \leqslant K_\rho \delta^{-2}\delta^{m_1(\rho)} \log\frac{1}{\delta} r^\rho \tag{2.12}$$

except for a set of z of radial measure not exceeding $\delta^{\frac{1}{2}}R$. Finally let $\varpi_2(z)$ be formed by replacing $z_{s,t}$ by $\zeta_{s,t}$ in $\Pi_2(z)$. Then

$$|\log|\varpi_2(z)| - \log|\Pi_2(z)|| \leqslant \sum_{s,t}\sum_{l=1}^{q} \left|\frac{z^l}{l}\left(\frac{1}{z_{s,t}^l} - \frac{1}{\zeta_{s,t}^l}\right)\right| + \sum_{s,t}\left|\log\left|1 - \frac{z(z_{s,t}-\zeta_{s,t})}{\zeta_{s,t}(z_{s,t}-z)}\right|\right|$$

$$\leqslant K(\rho)\sum_{s,t}\sum_{l=1}^{q}\frac{r^l}{r_s^{l+1}}|z_{s,t}-\zeta_{s,t}| + \sum_{s,t}\left|\log\left|1 - \frac{z(z_{s,t}-\zeta_{s,t})}{\zeta_{s,t}(z_{s,t}-z)}\right|\right|. \tag{2.13}$$

Moreover, if $\frac{1}{2}(1+\lambda)R \leqslant |z| \leqslant \dfrac{1}{2\lambda}(1+\lambda)R$ and $|z_{s,t}| \leqslant \lambda R$,

$$\left|\frac{z(z_{s,t}-\zeta_{s,t})}{\zeta_{s,t}(z_{s,t}-z)}\right| \leqslant \frac{\delta r_s^{1-\frac{1}{2}\rho}}{r_s}\left|\frac{z}{z_{s,t}-z}\right| \leqslant K\delta^{\frac{1}{2}} r_s^{-\frac{1}{2}\rho}$$

$$\leqslant \tfrac{1}{2}$$

if δ is small enough. Consequently

$$|\log|\Pi_2(z)| - \log|\varpi_2(z)|| \leqslant K_\rho \delta \sum_{s,t} r^q r_s^{-\frac{1}{2}\rho-q} + K\delta^{\frac{1}{2}}\sum_{s,t} r_s^{-\frac{1}{2}\rho}$$

$$\leqslant K_\rho \sum_{r_s \leqslant \lambda R}\left(\frac{r}{r_s}\right)^q + K\delta^{-\frac{1}{2}}\sum_{r_s\leqslant\lambda R} 1,$$

and, using Lemma 2 (i) to estimate these sums, we get

$$|\log|\Pi_2(z)| - \log|\varpi_2(z)|| = O(\delta^{-2}r^{\frac{1}{2}\rho}\log r). \tag{2.14}$$

Also, since

$$\left(\frac{r_s}{r}\right)^{n_s} \leqslant \left(\frac{1-\delta^{\frac{1}{2}}}{1-\frac{1}{2}\delta^{\frac{1}{2}}}\right)^{2\pi/\delta} \leqslant e^{-\pi},$$

we have

$$\log|\varpi_2(z)| = \sum_{r_s\leqslant\lambda R}\log\left|1-\left(\frac{z}{r_s}\right)^{n_s}\right|$$

$$= O(\delta^{-1}r^{\frac{1}{2}\rho}) + 2\pi\delta^{-1}\sum_{r_s\leqslant\lambda R} r_s^{\frac{1}{2}\rho}\log\frac{r}{r_s}$$

$$= O(\delta^{-1}r^{\frac{1}{2}\rho}) + 2\pi\delta^{-2}\sum_{r_s\leqslant\lambda R}(r_{s+1}-r_s)r_s^{\rho-1}\log\frac{r}{r_s}. \tag{2.15}$$

Inequalities (2.1) and (2.2) in the restricted range

$$\tfrac{1}{2}(1+\lambda)R \leqslant |z| \leqslant \frac{1}{2\lambda}(1+\lambda)R$$

follow from (2.12), (2.14), and (2.15), with an exceptional set of radial measure at most $\delta^{\frac{1}{2}}R$, by similar arguments to those used to derive (7.12) of (**2**) and we can extend them to $0 \leqslant |z| \leqslant R$ and derive (2.3) as in (**2**) 727.

3. We now proceed to the proof of Theorems B and C. Choose $\lambda, \nu > 0$ so that

$$\delta = 2(1+\lambda)(1+\nu)d < \left(\frac{2\pi}{\rho^2\kappa}\right)^{\frac{1}{2}} \tag{3.1}$$

and consider the Valiron dissection into quadrilaterals $Q_{s,t}$ of mesh δ. Let $Q'_{s,t}$ be the concentric† quadrilaterals of mesh $2\lambda d$. If E completely covers $Q'_{s,t}$, add to E all r for which $|z| = r$ meets $Q_{s,t}$ and let the new set thus obtained be E_1. If E_1 does not completely cover $Q_{s,t}$, choose $z'_{s,t}$ in $Q'_{s,t}$ so that $|z'_{s,t}|$ does not belong to E and $z_{s,t}$ such that

$$|f(z_{s,t})| = \inf_{|z-z'_{s,t}| \leqslant d|z'_{s,t}|^{1-\frac{1}{2}\rho}} |f(z)|. \tag{3.2}$$

Write $$\beta = \limsup |z_{s,t}|^{-\rho} \log|f(z_{s,t})|.$$

By the choice of the $Q'_{s,t}$ the set of $z_{s,t}$ satisfies the conditions of Lemma 3 for all sufficiently small h with Θ replaced by D^*E_1 where

$$D^*E_1 \leqslant \frac{\Lambda}{\lambda}(1+\lambda)(1+\nu). \tag{3.3}$$

If δ is sufficiently small, we can now apply Lemmas 1 and 3. Writing temporarily τ for $\tau_\rho\left\{\dfrac{\Lambda(1+\lambda)(1+\nu)}{\lambda}\right\}$ we conclude that there are positive constants $m(\rho)$ and K_ρ such that, if $f(z)$ is an integral function of order ρ and type $\kappa(f)$ with

$$\kappa(f) < \frac{2\pi}{\rho^2\delta^2}\left(1-\tau-K_\rho\,\delta^{m(\rho)}\log\frac{1}{\delta}\right), \tag{3.4}$$

then

$$\kappa(f) \leqslant \beta\left(1-\tau+K_\rho\,\delta^{m(\rho)}\log\frac{1}{\delta}\right)+\frac{2\pi}{\rho^2\delta^2}\left(1-(1-\tau)^2+K_\rho\,\delta^{m(\rho)}\log\frac{1}{\delta}\right). \tag{3.5}$$

By choice of $\{z'_{s,t}\}$ $$\beta \leqslant \mu,$$

† The centre of $Q_{s,t}$ is the point $\frac{1}{2}(r_s+r_{s+1})\exp i(t+\frac{1}{2})\delta'(s)$.

and thus (3.5) implies that, if δ is sufficiently small and (3.4) holds,

$$\mu\left(1-\tau+K_\rho\delta^{m(\rho)}\log\frac{1}{\delta}\right)\geqslant\beta\left(1-\tau+K_\rho\delta^{m(\rho)}\log\frac{1}{\delta}\right)$$
$$\geqslant\kappa(f)-\frac{2\pi}{\rho^2\delta^2}\left(2\tau-\tau^2+K_\rho\delta^{m(\rho)}\log\frac{1}{\delta}\right).$$

Letting $\nu\to 0$ we conclude that, if $(1+\lambda)d$ is sufficiently small,

$$\kappa d^2<\frac{\pi}{2\rho^2(1+\lambda)^2}\left[1-\tau_\rho\left\{\frac{\Lambda(1+\lambda)}{\lambda}\right\}-K_\rho d^{m(\rho)}\log\frac{1}{d}\right] \tag{3.6}$$

implies that

$$\mu d^2\left[1-\tau_\rho\left\{\frac{\Lambda(1+\lambda)}{\lambda}\right\}-K_\rho d^{m(\rho)}\log\frac{1}{d}\right]$$
$$\geqslant\kappa d^2-\frac{\pi}{2\rho^2(1+\lambda)^2}\left[2\tau_\rho\left\{\frac{\Lambda(1+\lambda)}{\lambda}\right\}-\tau_\rho^2\left\{\frac{\Lambda(1+\lambda)}{\lambda}\right\}+K_\rho d^{m(\rho)}\log\frac{1}{d}\right]. \tag{3.7}$$

We now write $z=L\zeta$, so that $f(z)$ is transformed into $g(\zeta)$ of type κL^ρ. It is easy to see that

$$D^*E(f,\kappa,\mu,d)=D^*E(g,\kappa L^\rho,\mu',d'),$$

where $\mu'=\mu L^\rho$ and $d'=dL^{-1+\rho}$ so that

$$\kappa d^2=\kappa L^\rho d'^2,\qquad \mu d^2=\mu' d'^2. \tag{3.8}$$

For fixed $\mu<\kappa$ and d we can apply the above argument to $E(g,\kappa L^\rho,\mu',d')$ if L is large enough and obtain (3.6) and (3.7) with d replaced by d'. As $L\to\infty$, $d'\to 0$ and the terms involving d' alone disappear, the inequalities being otherwise unaltered. We conclude that

$$\kappa d^2\leqslant\frac{\pi}{2\rho^2(1+\lambda)^2}\left[1-\tau_\rho\left\{\frac{\Lambda(1+\lambda)}{\lambda}\right\}\right] \tag{3.9}$$

implies that

$$\mu d^2\left[1-\tau_\rho\left\{\frac{\Lambda(1+\lambda)}{\lambda}\right\}\right]\geqslant\kappa d^2-\frac{\pi}{2\rho^2(1+\lambda)^2}\left[2\tau_\rho\left\{\frac{\Lambda(1+\lambda)}{\lambda}\right\}-\tau_\rho^2\left\{\frac{\Lambda(1+\lambda)}{\lambda}\right\}\right]$$
$$\geqslant\kappa d^2-\frac{\pi}{\rho^2(1+\lambda)^2}\tau_\rho\left\{\frac{\Lambda(1+\lambda)}{\lambda}\right\}; \tag{3.10}$$

(3.9) and (3.10) together imply that

$$\tau_\rho\left\{\frac{\Lambda(1+\lambda)}{\lambda}\right\}\geqslant\min\left\{1-\frac{2\rho^2(1+\lambda)^2d^2\kappa}{\pi},\frac{\kappa-\mu}{\pi\rho^{-2}d^{-2}(1+\lambda)^{-2}-\mu}\right\}. \tag{3.11}$$

So far λ is restricted only by the inequality $2\rho^2(1+\lambda)^2d^2\kappa<\pi$ and we could therefore choose it to secure the largest value of Λ. Since our

result is in any case not best-possible, we confine ourselves to striking a fairly obvious balance between λ small and $1-2\rho^2(1+\lambda)^2\kappa/\pi$ small by choosing $\lambda = \lambda_0$ so that

$$1-\frac{2\rho^2(1+\lambda_0)^2d^2\kappa}{\pi} = \frac{1}{2}\left(1-\frac{2\rho^2d^2\kappa}{\pi}\right). \tag{3.12}$$

Since
$$\frac{\pi}{\rho^2(1+\lambda_0)^2d^2}-\mu \geqslant 2\kappa-\mu \geqslant \kappa,$$

we obtain the result stated in Theorem C.

If $\rho > 1$, we can make use of the fact that

$$\tau_\rho(x) \leqslant \rho^2 x \max_{0\leqslant u\leqslant 1} u^{\rho-1}\log\frac{1}{u} = \frac{\rho^2}{e(\rho-1)}x$$

and conclude from (3.11) that

$$\Lambda = D^*E \geqslant \frac{\lambda_0}{1+\lambda_0}\frac{e(\rho-1)}{\rho^2}\min\left(\frac{1}{2}\left(1-\frac{2\rho^2d^2\kappa}{\pi}\right), 1-\frac{\mu}{\kappa}\right). \tag{3.13}$$

By the choice of λ_0

$$\begin{aligned}\frac{\lambda_0}{1+\lambda_0} &= 1-\left(\frac{2}{1+\pi/2\rho^2d^2\kappa}\right)^{\frac{1}{2}} \\ &= \left(1-\frac{2}{1+\pi/2\rho^2d^2\kappa}\right)\Big/\left\{1+\left(\frac{2}{1+\pi/2\rho^2d^2\kappa}\right)^{\frac{1}{2}}\right\}\end{aligned}$$

and, from the fact that $\dfrac{\pi}{2\rho^2d^2\kappa} > 1$,

$$\begin{aligned}\frac{\lambda_0}{1+\lambda_0} &\geqslant \frac{1}{2}\left(1-\frac{2\rho^2d^2\kappa}{\pi}\right)\Big/\left(1+\frac{2\rho^2d^2\kappa}{\pi}\right) \\ &\geqslant \frac{1}{4}\left(1-\frac{2\rho^2d^2\kappa}{\pi}\right).\end{aligned} \tag{3.14}$$

Theorem B follows from (3.13) and (3.14).

REFERENCES

1. B. J. Maitland, 'The flat regions of integral functions of finite order', *Quart. J. of Math.* (Oxford) 15 (1944), 84–96.
2. M. E. Noble, 'Non-measurable interpolation sets (I): Integral functions', *Proc. Cambridge Phil. Soc.* 47 (1951), 713–32.
3. —— 'Non-measurable interpolation sets (II): Functions regular in an angle', ibid. 47 (1951), 733–40.
4. G. Valiron, 'Recherches sur le théorème de M. Borel dans la théorie des fonctions méromorphes', *Acta Math.* 52 (1929), 67–92.
5. R. Rado, 'Some elementary Tauberian theorems (II)', *Quart. J. of Math.* (Oxford) 10 (1939), 28–37.

THE LOCATION OF SINGULARITIES ON THE CIRCLE OF CONVERGENCE OF GAP SERIES (I)

By F. W. PONTING (*Aberdeen*)

[Received 5 February 1952]

1. Introduction

We consider the functions

$$\phi(z) = \sum_0^\infty c_n z^n \tag{1}$$

which have exactly k different singularities (all isolated, non-critical, and of finite exponential order) on their circles of convergence. Macintyre and Wilson† have shown (M.W., 79, Theorem 6) that, if the upper density of small coefficients of $\phi(z)$ is greater than

$$(k-2)/(k-1),$$

then the singularities‡ are at the vertices of a k-sided regular polygon. In this case the density exists and is equal to $(k-1)/k$ and the singularities are virtually identical in form. [See M.W., 61, for the definition of 'small coefficients'.]

I consider only the case of k even and write $k = 2l$. This work is an extension of that in M.W. and depends on the argument from function-theory there developed in § 8 and § 6. In this paper I shall prove, for $k = 4$ and $k = 6$, the following theorem:

Theorem 1. *If the upper density of small coefficients in* (1) *is greater than* $1-1/l$, *then the singularities fall at* k *vertices of a regular polygon. This polygon has*

$$k \tag{2}$$

$$\text{(a)}\quad k+u, \qquad \text{(b)}\quad k+2u', \tag{3}$$

or

$$jl \tag{4}$$

sides, where u *divides* k, $3u' = k$, *and* j *is an integer greater than* 3.

In (3 a) the k singularities are located at the vertices of k/u regular u-agons, in (3 b) they are at the vertices of three regular u'-agons, and

† A. J. Macintyre and R. Wilson, 'Coefficient density and the distribution of singular points on the circle of convergence', *Proc. London Math. Soc.* (2), 47 (1940), 60–80. This paper will be referred to as M.W.

‡ The qualifying phrase 'on the circle of convergence' is to be understood here, and throughout this paper.

in (4) at those of two regular l-agons.† The general case (when k is even) will be considered in another paper.

When k is even, the function

$$\phi(z) = (1-\alpha z^l)^{-1}+(1-\beta z^l)^{-1} \quad (|\alpha| = |\beta|)$$

has a small coefficient density of $1-1/l$, and its singularities are at the vertices of two regular polygons. Since these can be independent, it follows that, when k is even, Theorem 1 is a best-possible result.

When k is odd and a multiple of 3, say $k = 3l'$, then

$$\phi(z) = (1-\alpha z^{l'})^{-1}+(1-\beta z^{l'})^{-1}+(1-\gamma z^{l'})^{-1} \quad (|\alpha| = |\beta| = |\gamma|)$$

has a small coefficient density of $1-1/l'$.

When k is odd, and not a multiple of 3,

$$\phi(z) = (1-\alpha z^{l''})^{-1}+(1-\beta z^{l''-1})^{-1} \quad (2l'' = k+1;\ |\alpha| = |\beta|)$$

has a small coefficient density of $1-2/l''$.

It might be conjectured that in these two cases the number $1-1/l$ of Theorem 1 could be replaced by $1-1/l'$ and $1-2/l''$ respectively, but there will be more types of polygons in such cases with consequent complications.

This conjecture certainly holds when $k = 3$, for then $l' = 1$, and it was shown in M.W. that, if the upper density of small coefficients was positive, then the singularities lay at three vertices of some regular polygon.

Small Latin letters (except a, c, e, h, i, and z) will denote non-negative integers.

As examples of the general case,

$\phi(z) = (1-z^k)^{-1}$ gives (2);

$\phi(z) = (1-z^u)(1-z^{k+u})^{-1}$ gives (3 a) when u divides k;

$\phi(z) = (1+Rz^u+z^{2u})(1-z^{5u})^{-1}$ gives (3 b) when $R^2 = R+1$ and $k = 3u$;

$\phi(z) = (1-z^j)^{-1}-\omega(1-\omega z^j)^{-1}$ gives (4) when ω is a primitive jth root of unity; the density of small coefficients being respectively

$$1-1/k, \quad (k+u-2)/(k+u), \quad (k+2u-3)/(k+2u), \quad 1-1/l+1/(jl).$$

The next section deals with any even k. The results are needed for $k = 4$ and $k = 6$, and there is not much simplification in taking these particular values.

2. When the upper density of small coefficients of (1) is greater than

† I take a single point to be a regular 1-agon and a pair of diametrically opposite points to be a regular 2-agon.

$1-1/l$, let it be greater than $1-1/l+\delta$, where δ is positive. Take

$$N > 3/(l\delta)$$

and divide the coefficients of (1) into consecutive sections of Nl coefficients, and divide each section into consecutive blocks of l coefficients.

In a section of Nl coefficients, which must occur with positive upper density, at least $Nl-N+Nl\delta$ are small, so that there are at most $N-Nl\delta$ non-small coefficients, i.e. at most $N-3$ non-small coefficients. Hence three at least of the blocks of l coefficients have only small coefficients. I denote such a block by **0**. Similarly, a block with exactly m non-small coefficients will be denoted by **m**. If one of the following distributions occurs, I say that there is a *favourable situation*.† These distributions are

(i) **0 0**,
(ii) **0 1 1 . . . 1 0**,
(iii) **0 1 0 1**,
(iv) **0 1 0 2 1 . . . 1 0**.

In (ii) there need only be two **1** blocks, and in (iv) there need not be any **1** blocks following the **2** block.

LEMMA 1. *If there are at most $M-3$ non-small coefficients in a section of Ml coefficients, then there is at least one favourable situation.*

Proof. I use induction. The lemma is clearly true for $M = 3$ and $M = 4$, for we always have (i). We assume that it is true for all $M \leqslant L-1$.

Consider a section of L blocks of l coefficients ($L \geqslant 5$). If the first block contains one or more non-small coefficients, we have at most $L-4$ non-small coefficients in the remaining $L-1$ blocks, and hence there is a favourable situation. Thus we may take the first block to be a **0** block.

If the second contains more than one non-small coefficient, omit the first two blocks, and we again have a favourable situation. If the second is a **0** block, we have (i). Similar arguments show that we are left to consider the first three blocks as

0 1 0 or **0 1 1**.

If we then have **0 1 0 0** or **0 1 0 1**, we have (i) or (iii) respectively; if the fourth block contains more than two non-small coefficients, then the remaining $L-4$ blocks can contain $L-7$ non-small coefficients at most, and we have a favourable situation. We have to consider

0 1 0 2.

† The reasons for this choice will become clear later.

If the fifth block is a **0** block, we have (iv); if the fifth block contains more than one non-small coefficient, we omit the first five blocks, and must have a favourable situation in the remainder.† So we take

0 1 0 2 1;

arguing in a similar manner we have either (iv) or

0 1 0 2 1 1 . . . 1.

However, with this distribution, there is still a deficiency of 2 and so we must come to a **0** block, and hence get (iv). A similar argument shows that

0 1 1

also leads to a favourable situation.

The lemma follows by the principle of induction.

Suppose that a section of Nl coefficients, with $N-3$ at most non-small, occurs with upper density $\rho > 0$. Then there is at least one favourable situation in this section, and the number of favourable situations is certainly less than $(Nl)^{Nl}$. Thus there exists a favourable situation with an upper density greater than $\rho(Nl)^{-Nl}$. Hence we have

THEOREM 2. *If the upper density of small coefficients of* (1) *is greater than* $1-1/l$, *then a favourable situation occurs with a positive upper density.*

It was shown in M.W. (79) that k consecutive coefficients cannot all be small, except for a sequence of density zero. This disposes of (i) since each of the two blocks has l elements with $k = 2l$.

Let c_{n+1} be the first coefficient of a favourable situation of Theorem 2, and let

$$c_{n+p},\ c_{n+q},\ c_{n+r},\ c_{n+s}$$

be the first four non-small coefficients. Then we have from (i)–(iv) and the above,

$$l < p \leqslant 2l < q, \qquad 3l < r, \qquad 4l < s,$$

and

$$q-p \leqslant k, \qquad r-q \leqslant k, \qquad s-r \leqslant k.$$

I construct from the $k \times Nl$ matrix

$$(\exp(-i\tau\alpha_\sigma)) \quad (\sigma = 1, 2, \ldots, k;\ \tau = 1, 2, \ldots, Nl), \tag{5}$$

where the k singularities are at the points $c\exp(i\alpha_\sigma)$ of the circle of convergence of (1), a k-rowed matrix:

$$A \tag{6}$$

by omitting columns p, q, r, s, and all other columns of (5) which corre-

† For there is still a deficiency of at least 3 between the number of blocks and the number of non-small coefficients.

spond to non-small coefficients. As in M.W., § 8, it follows that all kth order minors of (6) vanish, and this forms the logical basis of the succeeding arguments. We shall need the well-known†

LEMMA 2. *If* $(\lambda_1, \lambda_2, \ldots, \lambda_k)$ *and* $(\mu_1, \mu_2, \ldots, \mu_k)$ *are conjugate partitions of* $\sum \lambda_j$ *and* a_m, h_m *are the m-th elementary and m-th homogeneous symmetric functions respectively of* $\theta_1, \theta_2, \ldots, \theta_k$,‡ *where* $\theta_m \neq \theta_n$ *if* $m \neq n$, *then*

$$|\theta_\sigma^{\tau-1+\lambda_{k-\tau+1}}|/|\theta_\sigma^{\tau-1}| = |h_{\tau-\sigma+\lambda_\sigma}| = |a_{\tau-\sigma+\mu_\sigma}| \quad (\sigma, \tau = 1, 2, \ldots, k).$$

We use the convention that $a_j = 0$ if $j < 0$ or $j > k$, $h_j = 0$ if $j < 0$, and $a_0 = h_0 = 1$.

3. When $k = 4$, I show that the singularities of (1) must lie at four vertices of a regular polygon with 4, 5, 6, or $2j$ sides.

We now take the singularities of (1) to be at the zeros of

$$F(z) = a_0 - a_1 z + a_2 z^2 - a_3 z^3 + a_4 z^4 \quad (a_0 = a_4 = 1). \tag{7}$$

We also take the circle of convergence of (1) to be the unit circle and rotate the z-plane so that $a_4 = 1$. Evidently this involves no loss of generality. Since from (5) the singularities of (1) are at $\exp(i\alpha_\sigma)$, where $\sigma = 1, 2, 3, 4$, these points are the zeros of (7), and so

$$a_l = \bar{a}_{k-l} = \sum \exp(-i\alpha_1)\exp(-i\alpha_2)\ldots\exp(-i\alpha_l), \tag{8}$$

where the bar denotes the complex conjugate. We make frequent use of (8) in the succeeding calculations.

Of the favourable situations of Theorem 2 we need only consider situation (ii). For (i) is impossible, and **0 1 0** alone gives

$$c_{n+1}, c_{n+2}, c_{n+4}, c_{n+5}, c_{n+6} \quad \text{or} \quad c_{n+1}, c_{n+2}, c_{n+3}, c_{n+5}, c_{n+6}$$

all small for a sequence of n of positive upper density. These distributions will be denoted by§

$$0\,0,\ 1\,0,\ 0\,0 \quad \text{and} \quad 0\,0,\ 0\,1,\ 0\,0 \quad \text{respectively.}$$

The methods of M.W. give $a_1 = a_2 = a_3 = 0$ in both cases, and we have (2).

† Cf. D. E. Littlewood, *Theory of Group Characters* (Oxford, 1940), chap. vi, equations (6.3.1), (6.3.2), and (6.3.3). The order of the columns of both determinants is in the reverse order to that used by Littlewood.

‡ We put $\theta_j = \exp(-i\alpha_j)$ for convenience in printing and note that the θ_j are all different.

§ I use '1' to denote a non-small coefficient, and '0' to denote a small coefficient. The use of this notation will imply that the particular distribution occurs with a positive upper density.

Taking the first three blocks, each containing two coefficients, there remain the possibilities

(*a*) 0 0, 0 1, 0 1, (*b*) 0 0, 0 1, 1 0,

(*c*) 0 0, 1 0, 0 1, (*d*) 0 0, 1 0, 1 0.

3.1. *Distribution* (*a*). As in M.W., we have $a_1 = a_3 = 0$.

From Theorem 2, the $(2j+2)$th coefficient in situation (ii) will be small, for some j. Hence columns 1, 2, 3, and $2j+2$ of (5) are retained in (6). So that

$$\begin{vmatrix} \theta_1 & \theta_1^2 & \theta_1^3 & \theta_1^{2j+2} \\ \theta_2 & \theta_2^2 & \theta_2^3 & \theta_2^{2j+2} \\ \theta_3 & \theta_3^2 & \theta_3^3 & \theta_3^{2j+2} \\ \theta_4 & \theta_4^2 & \theta_4^3 & \theta_4^{2j+2} \end{vmatrix} = 0, \text{ i.e. } \begin{vmatrix} 1 & \theta_1 & \theta_1^2 & \theta_1^{2j+1} \\ 1 & \theta_2 & \theta_2^2 & \theta_2^{2j+1} \\ 1 & \theta_3 & \theta_3^2 & \theta_3^{2j+1} \\ 1 & \theta_4 & \theta_4^2 & \theta_4^{2j+1} \end{vmatrix} = 0.$$

Then,† in Lemma 2, $\lambda_4 = \lambda_3 = \lambda_2 = 0$, $\lambda_1 = 2j-2$, hence

$$\begin{vmatrix} h_{2j-2} & h_{2j-1} & h_{2j} & h_{2j+1} \\ 0 & 1 & h_1 & h_2 \\ 0 & 0 & 1 & h_1 \\ 0 & 0 & 0 & 1 \end{vmatrix} = 0,$$

i.e. $h_{2j-2} = 0$.

It is well known that

$$(1-a_1 z+a_2 z^2-+\ldots+(-1)^k a_k z^k)^{-1} = \sum h_l z^l.$$

Since $a_1 = 0 = a_3$, in this case we have

$$1+a_2 z^2+z^4 = (1-\delta_1 z^2)(1-\delta_2 z^2)$$

where $\delta_1 \neq \delta_2$, and so

$$\sum h_l z^l = (1+a_2 z^2+z^4)^{-1} = (\delta_1-\delta_2)^{-1}[\delta_1(1-\delta_1 z^2)^{-1}-\delta_2(1-\delta_2 z^2)^{-1}].$$

Hence $\delta_1^j = \delta_2^j$, and we have (4), or (3 a) with $u = 2$ when $j = 3$.

3.2. *Distribution* (*b*). Columns 1, 2, 3, and 6 of (5) give $h_2 = 0$, i.e. $a_1^2 = a_2$.

3.21. If we have

0 0, 0 1, 1 0, 0 1 or 0 0, 0 1, 1 0, 0 0,

we find as in 3.1 that $h_3 = 0$ and thus $a_1^3 = a_3$ from the well-known relations

$$h_1-a_1 = 0, \qquad h_2-a_1 h_1+a_2 = 0, \qquad h_3-a_1 h_2+a_2 h_1-a_3 = 0.$$

But, from (8), $\bar{a}_3 = a_1$ so that $a_1^4 = 1$, and (7) takes the form

$$F(z) = 1-\omega z+\omega^2 z^2-\omega^3 z^3+z^4 = (1-\omega z)^{-1}(1-\omega z^5),$$

† If columns $p_1, p_2, \ldots, p_k$ of (5) are retained in (6), then we find, after removing non-zero factors, that $\lambda_{k+1-t} = p_t-(p_1+t-1)$.

where $\omega^4 = 1$. Thus the singularities lie at four vertices of a pentagon, and we have (3 a) with $u = 1$.

3.22. If we have 0 0, 0 1, 1 0, 1 0,

then $h_4 = 0$. Now $h_3 = a_3 - a_1^3$, since $h_2 = 0$ from § 3.2, and from

$$h_4 - a_1 h_3 + a_2 h_2 - a_3 h_1 + a_4 = 0,$$

we have $$a_1^4 - 2a_1 a_3 + 1 = 0.$$

Put $a_1 = Re^{i\theta}$ (R, θ real); then

$$R^4 e^{4i\theta} - 2R^2 + 1 = 0.$$

Now, from § 3.2, $a_1^2 = a_2 = \bar{a}_2 = \bar{a}_1^2$; hence $e^{4i\theta} = 1$ and thus $R = \pm 1$. Hence $a_1^4 = 1$ and $a_3 = a_1^3$, and we obtain (3 a) as in § 3.21 since $a_1^2 = a_2$ from § 3.2.

3.3. *Distribution* (*c*). Columns 1, 2, 4, 5 of (5) give $a_2 = 0$.

3.31. If we have

0 0, 1 0, 0 1, 0 1 or 0 0, 1 0, 0 1, 0 0,

then columns 2, 4, 5, 7 of (5) give†

$$\begin{vmatrix} a_3 & a_4 \\ 1 & a_1 \end{vmatrix} = 0,$$

so that $$a_1 a_3 = a_4.$$

3.32. If we have 0 0, 1 0, 0 1, 1 0,

then columns 2, 4, 5, 8 of (5) give

$$\begin{vmatrix} a_3 & a_4 & a_5 \\ 1 & a_1 & a_2 \\ 0 & 1 & a_1 \end{vmatrix} = 0,$$

so that, since $a_2 = 0 = a_5$,

$$a_1(a_1 a_3 - a_4) = 0.$$

If $a_1 = 0$, then $\bar{a}_3 = 0$ and, since $a_2 = 0$ from § 3.3, (2) follows.

We are left in all other cases of (*c*) with

$$a_1 a_3 = a_4.$$

Since, from § 3.3, $a_2 = 0$, equation (7) becomes‡

$$F(z) = (1 - a_1 z)(1 - a_3 z^3). \tag{9}$$

† We find that $\lambda_4 = 0, \lambda_3 = \lambda_2 = 1, \lambda_1 = 2$. The partition conjugate to (2, 1, 1, 0) is (3, 1, 0, 0).

‡ It can be shown that if every third coefficient of (1) is non-small, then all fourth-order minors of (6) are zero when $a_2 = 0$ and $a_1 a_3 = 1$. Thus we cannot obtain any more information algebraically.

If we put $a_3 = \lambda^{-1}$, then $\lambda^4 \neq 1$ (otherwise the singularities are not distinct), and the singularities are at

$$z = \lambda^{\frac{1}{3}},\ \omega\lambda^{\frac{1}{3}},\ \omega^2\lambda^{\frac{1}{3}},\ \lambda^{-1},$$

where ω is a primitive cube root of unity.

Consider the three functions

$$\phi_m(z) = \tfrac{1}{3}\{\phi(z)+\omega^{-m}\phi(\omega z)+\omega^{-2m}\phi(\omega^2 z)\} \quad (m = 0, 1, 2) \qquad (10)$$
$$= \sum_j c_{m+3j} z^{m+3j}.$$

Each $\phi_m(z)$ will have six singularities at most, at

$$\lambda^{-1},\ \omega\lambda^{-1},\ \omega^2\lambda^{-1},\ \lambda^{\frac{1}{3}},\ \omega\lambda^{\frac{1}{3}},\ \omega^2\lambda^{\frac{1}{3}}, \qquad (11)$$

and the first three of these must remain (although the last three may cancel).

Now the lower density of non-small coefficients of $\phi(z)$ is less than $\frac{1}{2}$; hence the lower density of non-small coefficients of at least one $\phi_m(z)$ is less than $\frac{1}{6}$, but this is possible only when this $\phi_m(z)$ has no singularities. Hence we have a contradiction, and (9) is impossible.

3.4. *Distribution* (*d*). Columns 1, 2, 4, 6 of (5) give

$$\begin{vmatrix} a_2 & a_3 \\ 1 & a_1 \end{vmatrix} = 0,$$

so that $$a_1 a_2 = a_3. \qquad (12)$$

3.41. If we have 0 0, 1 0, 1 0, 0 1,

then columns 1, 2, 4, 7 of (5) give

$$\begin{vmatrix} a_2 & a_3 & a_4 \\ 1 & a_1 & a_2 \\ 0 & 1 & a_1 \end{vmatrix} = 0,$$

which, with (12), gives $$\begin{vmatrix} a_2 & a_4 \\ 1 & a_2 \end{vmatrix} = 0,$$

so that $$a_2^2 = 1. \qquad (13)$$

If the fifth block is now 0 0 or 0 1, columns 4, 6, 7, 9 of (5) give

$$\begin{vmatrix} a_3 & a_4 \\ 1 & a_1 \end{vmatrix} = 0,$$

so that $$a_1 a_3 = 1. \qquad (14)$$

From (12), (13), and (14) we have either

$$a_2 = 1, \qquad a_1 = a_3 = \pm 1,$$

or $$a_2 = -1, \qquad a_1 = -a_3 = \pm i.$$

In each case, (7) becomes

$$F(z) = (1-\omega z+\omega^2 z^2-\omega^3 z^3+\omega^4 z^4) \quad (\omega^4 = 1);$$

and we have (3 a) as in § 3.21.

So we now consider

$$0\,0,\ 1\,0,\ 1\,0,\ 0\,1,\ 1\,0.$$

If the sixth block is 0 0 or 0 1, then columns 6, 7, 10, 11 of (5) give

$$\begin{vmatrix} a_2 & a_3 \\ a_1 & a_2 \end{vmatrix} = 0,$$

so that

$$a_2^2 = a_1 a_3$$

and from (13) we have (14), and thus (3 a) follows as above.

If the sixth block is 1 0, then columns 6, 7, 10, 12 of (5) give

$$\begin{vmatrix} a_2 & a_3 & a_4 \\ a_1 & a_2 & a_3 \\ 0 & 1 & a_1 \end{vmatrix} = 0,$$

so that $a_1(a_2^2-a_1 a_3) = 0$, for from (12) and (13), $a_2 a_3 = a_1$. If $a_2^2 = a_1 a_3$, then, since $a_2^2 = 1$, we have (3 a) as above. If $a_1 = 0$, then (13) gives us (3 a).

3.42. If we have 0 0, 1 0, 1 0, 1 0 or 0 0, 1 0, 1 0, 0 0, then columns 2, 4, 6, 8 of (5) give

$$\begin{vmatrix} a_3 & a_4 & 0 \\ a_1 & a_2 & a_3 \\ 0 & 1 & a_1 \end{vmatrix} = 0.$$

Using (12), we find that

$$\begin{vmatrix} a_3 & a_4 & 0 \\ a_1 & 0 & 0 \\ 0 & 1 & a_1 \end{vmatrix} = 0,$$

so that $a_1 = 0$. We then argue as in § 3.1.

4. When $k = 6$, I show that the singularities of (1) must lie at six vertices of a regular polygon with 6, 7, 8, 9, 10, or $3j$ sides. Equation (7) is now replaced by

$$F(z) = 1-a_1 z+a_2 z^2-a_3 z^3+a_4 z^4-a_5 z^5+z^6 \quad (a_6 = 1); \qquad (15)$$

and (8) still holds.

If we have 0 0 0, 1 0 0, 0 0 0 or 0 0 0, 0 0 1, 0 0 0, it follows at once that

$$a_1 = a_2 = a_3 = a_4 = a_5 = 0, \qquad (16)$$

and hence (2) results.

We have thus to consider

(*a*)	0 0 0, 0 1 0, 0 0 0,	(*f*)	0 0 0, 0 1 0, 0 1 0,
(*b*)	0 0 0, 1 0 0, 1 0 0,	(*g*)	0 0 0, 0 1 0, 0 0 1,
(*c*)	0 0 0, 1 0 0, 0 1 0,	(*h*)	0 0 0, 0 0 1, 1 0 0,
(*d*)	0 0 0, 1 0 0, 0 0 1,	(*i*)	0 0 0, 0 0 1, 0 1 0,
(*e*)	0 0 0, 0 1 0, 1 0 0,	(*j*)	0 0 0, 0 0 1, 0 0 1.

Case (*a*) is the remaining distribution for situation (iii) and (iv), and will have one, or two, non-small coefficients in the fourth block. The remaining cases belong to situation (ii).

4.1. *Distribution* (*a*). We have

$$a_2 = a_3 = a_4 = 0. \tag{17}$$

If the fourth block† is 0 0 1 or 0 1 0 or 0 1 1, then (16) follows.

4.11. If we have 0 0 0, 0 1 0, 0 0 0, 1 0 0, or 0 0 0, 0 1 0, 0 0 0, 1 0 1, then columns 4, 6, 7, 8, 9, 11 of (5) give

$$\begin{vmatrix} a_5 & a_6 \\ 1 & a_1 \end{vmatrix} = 0,$$

so that

$$a_1 a_5 = a_6. \tag{18}$$

Equation (15) becomes

$$F(z) = (1-a_1 z)(1-a_5 z^5),$$

which is impossible by an argument like that of § 3.32.

4.12. If we have 0 0 0, 0 1 0, 0 0 0, 1 1 0, then columns 4, 6, 7, 8, 9, 12 of (5) give

$$\begin{vmatrix} a_5 & a_6 & 0 \\ 1 & a_1 & a_2 \\ 0 & 1 & a_1 \end{vmatrix} = 0.$$

Since $a_2 = 0$ and (18) is impossible, we have $a_1 = 0$, and hence (2) follows.

4.2. *Distribution* (*b*). Columns 1, 2, 3, 5, 6, 8 and 1, 2, 3, 5, 6, 9 of (5) give

$$\begin{vmatrix} a_3 & a_4 \\ 1 & a_1 \end{vmatrix} = 0 \quad \text{and} \quad \begin{vmatrix} a_3 & a_4 & a_5 \\ 1 & a_1 & a_2 \\ 0 & 1 & a_1 \end{vmatrix} = 0$$

respectively, so that

$$a_1 a_3 = a_4, \qquad a_2 a_3 = a_5. \tag{19}$$

Then $\bar{a}_2 \bar{a}_3 = \bar{a}_5$, and (8) gives $a_4 a_3 = a_1$. Hence

$$a_4 a_3^2 = a_4. \tag{20}$$

† We note that the case of a block 0 0 0 is covered by the discussion of any of 1 0 0, 0 1 0, or 0 0 1.

If $a_4 = 0$, (8) and (19) give

$$a_2 = a_1 = a_5 = 0. \tag{21}$$

In this case, some c_{n+3j+1} will be small, and, as in § 3.1, we find that if

$$(1-\delta_1 z^3)(1-\delta_2 z^3) = 1-a_3 z^3+z^6,$$

then $$\delta_1^t = \delta_2^t$$

for some t, and we have (4) or (3 a).

We now take the alternative in (20)

$$a_3^2 = 1. \tag{22}$$

4.21. If we have 0 0 0, 1 0 0, 1 0 0, 1 0 0 or 0 0 0, 1 0 0, 1 0 0, 0 0 1, then columns 1, 2, 3, 5, 6, 11 of (5) give

$$\begin{vmatrix} a_3 & a_4 & a_5 & a_6 & 0 \\ 1 & a_1 & a_2 & a_3 & a_4 \\ 0 & 1 & a_1 & a_2 & a_3 \\ 0 & 0 & 1 & a_1 & a_2 \\ 0 & 0 & 0 & 1 & a_1 \end{vmatrix} = 0.$$

Subtract a_3 times row 2 from row 1 and using (22) and (19) we get a new first row $0, 0, 0, 0, -a_3 a_4$. Hence $a_4 = 0$. This has been considered in (21).

4.22. If we have 0 0 0, 1 0 0, 1 0 0, 0 1 0, then columns 5, 6, 8, 9, 10, 12 of (5) give

$$\begin{vmatrix} a_4 & a_5 \\ 1 & a_1 \end{vmatrix} = 0,$$

so that $$a_1 a_4 = a_5. \tag{23}$$

From (19) we have $$a_1^2 a_3 = a_5 = a_2 a_3,$$

so that, from (22), $$a_1^2 = a_2. \tag{24}$$

From (23) and (8) we have

$$a_1 = a_5 a_2 = a_1 a_4 a_2.$$

If $a_1 = 0$, (19) gives $a_4 = 0$, which has been considered already in (21); hence we take

$$a_2 a_4 = 1. \tag{25}$$

From (19) and (25), $a_1 a_2 a_3 = a_2 a_4 = 1$ and, from (22) and (24), $a_1^3 = a_3$, and so (19), (22), and (24) give

$$a_j = \omega^j \quad (j = 1, 2, \ldots, 6;\ \omega^6 = 1).$$

Equation (15) then takes the form

$$F(z) = (1-\omega z)^{-1}(1-\omega z^7),$$

and we have (3 a) with $u = 1$.

4.3. *Distribution* (*c*). We have

$$a_3 = 0, \qquad a_5 = a_1 a_4, \tag{26}$$

from columns 1, 2, 3, 5, 6, 7 and 2, 3, 5, 6, 7, 9 respectively of (5).

4.31. If we have

$$0\,0\,0,\ 1\,0\,0,\ 0\,1\,0,\ 1\,0\,0,$$

then columns 5, 6, 7, 9, 11, 12 of (5) give

$$\begin{vmatrix} a_3 & a_4 \\ a_1 & a_2 \end{vmatrix} = 0,$$

so that $a_1 a_4 = 0$ since $a_3 = 0$ from (26).

If $a_4 = 0$, then $a_5 = 0$ from (26), and thus we have (2).

Hence we take

$$a_1 = 0. \tag{27}$$

Columns 2, 3, 5, 6, 7, 12 of (5) give

$$\begin{vmatrix} a_4 & a_5 & a_6 & 0 & 0 \\ 1 & a_1 & a_2 & a_3 & a_4 \\ 0 & 1 & a_1 & a_2 & a_3 \\ 0 & 0 & 1 & a_1 & a_2 \\ 0 & 0 & 0 & 1 & a_1 \end{vmatrix} = 0.$$

Using (26) and (27) we have

$$a_2(a_6 - a_4 a_2) = -a_4^2. \tag{28}$$

Put $a_2 = Re^{i\theta}$ (R, θ real); then $a_4 = Re^{-i\theta}$, and (28) becomes

$$R(1-R^2) = -R^2 e^{-3i\theta}.$$

Hence $a_2 = R\omega$ ($\omega^3 = 1$). If $R = 0$, we have (2), as above. Thus we consider

$$R^2 = R+1,$$

and now (15) becomes

$$F(z) = (1+R\omega z^2+R\omega^2 z^4+z^6) = (1-R\omega z^2+\omega^2 z^4)^{-1}(1+\omega^2 z^{10}).$$

This gives (3 b).

4.32. If we have

$$0\,0\,0,\ 1\,0\,0,\ 0\,1\,0,\ 0\,1\,0,$$

then columns 5, 6, 7, 9, 10, 12 of (5) give $a_4 = a_1 a_3$, so that from (26)

$$a_4 = 0, \qquad a_5 = 0.$$

However, columns 2, 3, 5, 6, 7, 10 of (5) give

$$\begin{vmatrix} a_4 & a_5 & a_6 \\ 1 & a_1 & a_2 \\ 0 & 1 & a_1 \end{vmatrix} = 0, \tag{29}$$

so that $a_6 = 0$, and this distribution is impossible.

4.33. If we have

$$0\,0\,0,\ 1\,0\,0,\ 0\,1\,0,\ 0\,0\,1,$$

then columns 2, 3, 5, 6, 7, 10 of (5) give (29). Using (26) it follows that $a_2 a_4 = 1$.

Since, from (26), $a_3 = 0$, (15) becomes

$$F(z) = (1-a_1 z+a_2 z^2)(1+a_4 z^4).$$

The zeros of this will be at

$$\lambda^{\frac{1}{4}},\ i\lambda^{\frac{1}{4}},\ -\lambda^{\frac{1}{4}},\ -i\lambda^{\frac{1}{4}},\ \lambda_1,\ \lambda_2, \tag{30}$$

where $$-\lambda^{-1} = a_4,$$

and λ_1, λ_2 are the roots of

$$1-a_1 z+a_2 z^2 = 0.$$

I define

$$\phi_m(z) = \tfrac{1}{4}\sum_{j=1}^{4} i^{-mj}\phi(i^j z) = \sum_{j=0}^{\infty} c_{m+4j} z^{m+4j} \quad (m = 0, 1, 2, 3). \tag{31}$$

Then each $\phi_m(z)$ can have twelve singularities at most. If it has any, then the lower density of non-small coefficients must be at least $\frac{1}{12}$.

Now $$\phi(z) = \phi_0(z)+\phi_1(z)+\phi_2(z)+\phi_3(z).$$

Hence at least one of the $\phi_m(z)$ must have no singularities; otherwise we should have the contradiction that the lower density of non-small coefficients of $\phi(z)$ would be at least $\frac{1}{3}$.

Let $\phi_{m_1}(z)$ have no singularities.

The singularities of $\phi_{m_1}(z)$ at

$$\pm\lambda_1,\ +i\lambda_1,\ \pm\lambda_2,\ \pm i\lambda_2$$

can vanish only if they cancel in pairs. Hence

$$\omega\lambda_1 = \lambda_2 \quad (\omega^4 = 1).$$

The possible singularities are now reduced to eight, and a second $\phi_m(z)$ must be without any. This is possible only if

$$\lambda_1 = -\lambda_2.$$

For, if $\lambda_2 = i\lambda_1$, then $\phi(z)$ and $\phi(iz)$, but not $\phi(-z)$ or $\phi(-iz)$, have singularities at $z = \lambda_1$. If two of the $\phi_m(z)$ have no singularities, then two of the functions

$$\phi(z)\pm\phi(iz), \qquad \phi(z)\pm i\phi(iz)$$

have no singularity at $z = \lambda_1$. This implies the contradiction that $\phi(z)$ has no singularity at this point.

A similar argument shows that we cannot have a third $\phi_m(z)$ without singularities. However, one of the two remaining $\phi_m(z)$ must have a

lower density of non-small coefficients less than $\frac{1}{6}$. Hence one only of

$$c_{m_3+4j-4},\ c_{m_3+4j},\ c_{m_3+4j+4}$$

can be non-small for a sequence of j of positive upper density. This must be the middle one since the function has eight singularities at most. Thus we have the distribution

$$1,\ 0\,0\,0\,0,\ 0\,0\,0\,1,\ 0\,0\,0\,0$$

and must have eight singularities which will lie at the vertices of a regular octagon. Since $\lambda_1 = -\lambda_2$, the six singularities of $\phi(z)$ are at six of these vertices, the omitted pair being diametrically opposite. This gives (3 a) with $u = 2$.

4.4. *Distribution* (*d*). We have

$$a_3 = a_4 = a_2 = 0. \tag{32}$$

If the fourth block is 0 1 0 or 0 0 1, then columns 3, 5, 6, 7, 8, 10 of (5) give $a_1 a_5 = a_6$. This situation is impossible as in § 4.11. We are left with

$$0\,0\,0,\ 1\,0\,0,\ 0\,0\,1,\ 1\,0\,0.$$

Then columns 3, 5, 6, 7, 8, 11 of (5) give

$$\begin{vmatrix} a_5 & a_6 & 0 \\ 1 & a_1 & a_2 \\ 0 & 1 & a_1 \end{vmatrix} = 0.$$

Then (32) gives $a_1(a_1 a_5 - a_6) = 0$. Hence $a_1 = 0$, and we have (2) (cf. § 4.12).

4.5. *Distribution* (*e*). Columns 1, 2, 3, 4, 6, 8 and 1, 2, 3, 4, 6, 9 of (5) give

$$a_3 = a_1 a_2, \qquad a_4 = a_2^2. \tag{33}$$

From (8), $a_2 = a_4^2 = a_2^4$, and thus $a_2 = 0$ or $a_2^3 = 1$.

4.51. If $a_2 = 0$, then $a_3 = 0$ from (33). If the fourth block is 1 0 0 or 0 0 1, then columns 1, 2, 3, 4, 6, 11 of (5) give

$$\begin{vmatrix} a_2 & a_3 & a_4 & a_5 & a_6 \\ 1 & a_1 & a_2 & a_3 & a_4 \\ 0 & 1 & a_1 & a_2 & a_3 \\ 0 & 0 & 1 & a_1 & a_2 \\ 0 & 0 & 0 & 1 & a_1 \end{vmatrix} = 0, \tag{34}$$

and so

$$a_1 a_5 = a_6. \tag{35}$$

This situation is impossible as in § 4.11.

If the fourth block is 0 1 0, then columns 1, 2, 3, 4, 6, 10 of (5) give, with (33),

$$a_5 = a_2 a_3 = 0.$$

This gives (2).

4.52. If $a_3^2 = 1$, then from (33),

$$a_2 a_4 = 1 = a_6, \tag{36}$$

and (8) and (33) give $a_3 = \bar{a}_3 = a_5 a_4 = a_5 a_2^2$ so that

$$a_5 = a_2 a_3. \tag{37}$$

If the fourth block is 1 0 0 or 0 1 0, then columns 1, 2, 3, 4, 6, 12 of (5) give

$$\begin{vmatrix} a_2 & a_3 & a_4 & a_5 & a_6 & 0 \\ 1 & a_1 & a_2 & a_3 & a_4 & a_5 \\ 0 & 1 & a_1 & a_2 & a_3 & a_4 \\ 0 & 0 & 1 & a_1 & a_2 & a_3 \\ 0 & 0 & 0 & 1 & a_1 & a_2 \\ 0 & 0 & 0 & 0 & 1 & a_1 \end{vmatrix} = 0. \tag{38}$$

Subtract a_2 times row 2 from row 1 of (38). Then, from (33), (36), (37),

$$a_2 a_5 = 0.$$

Hence $a_5 = 0$, and we have (3 a) since $a_1 = a_3 = a_5 = 0$ from (8) and (33), and so

$$F(z) = 1+\omega^2 z^2+\omega^4 z^4+z^6 = (1-\omega^2 z^8)(1-\omega^2 z^2)^{-1} \quad (\omega^6 = 1).$$

Hence we consider

$$0\,0\,0,\ 0\,1\,0,\ 1\,0\,0,\ 0\,0\,1.$$

If the fifth block is 0 1 0 or 0 0 1, columns 6, 8, 9, 10, 11, 13 of (5) give

$$a_5 a_1 = a_6. \tag{39}$$

Hence, from (33) and (37), $a_1^2 = a_2$ and we have (3 a) since $a_3 = a_1^3$ from (33).

If the fifth block is 1 0 0, then columns 8, 9, 10, 11, 14, 15 of (5) give

$$\begin{vmatrix} a_2 & a_3 \\ a_1 & a_2 \end{vmatrix} = 0$$

and again $a_1^2 = a_2$ from (33).

4.6. *Distribution* (f). We have

$$a_2 = 0, \qquad a_4 = a_1 a_3 \tag{40}$$

from columns 1, 2, 3, 4, 6, 7 and 2, 3, 4, 6, 7, 9 respectively of (5).

If $a_3 \neq 0$, then $a_1 = 0$, and the argument of § 4.2 gives (4) or (3 a). So we take

$$a_3 = 0.$$

If the fourth block is 0 1 0 or 0 0 1, then columns 2, 3, 4, 6, 7, 10 of (5) give

$$\begin{vmatrix} a_3 & a_4 & a_5 \\ 1 & a_1 & a_2 \\ 0 & 1 & a_1 \end{vmatrix} = 0.$$

Hence $a_5 = 0$, and we have (2). So we consider 0 0 0, 0 1 0, 0 1 0, 1 0 0. Then columns of 2, 3, 4, 6, 7, 11 of (5) give

$$\begin{vmatrix} a_3 & a_4 & a_5 & a_6 \\ 1 & a_1 & a_2 & a_3 \\ 0 & 1 & a_1 & a_2 \\ 0 & 0 & 1 & a_1 \end{vmatrix} = 0, \text{ i.e. } \begin{vmatrix} 0 & 0 & a_5 & a_6 \\ 1 & a_1 & 0 & 0 \\ 0 & 1 & a_1 & 0 \\ 0 & 0 & 1 & a_1 \end{vmatrix} = 0,$$

so that $a_1 a_5 = a_6$, which gives the impossible situation of § 4.11.

4.7. *Distribution* (g). We have

$$a_2 = a_3 = a_4 = 0. \tag{41}$$

If the fourth block is 0 1 0 or 0 0 1, then columns 3, 4, 6, 7, 8, 10 of (5) give $a_1 a_4 = a_5$, so that $a_5 = 0$ and we have (2). If the fourth block is 1 0 0, then columns 3, 4, 6, 7, 8, 11 of (5) give

$$\begin{vmatrix} a_4 & a_5 & a_6 \\ 1 & a_1 & a_2 \\ 0 & 1 & a_1 \end{vmatrix} = 0,$$

and from (41) we have $a_1 a_5 = a_6$ which is again impossible as in § 4.11.

4.8. *Distribution* (h). We have

$$h_2 = 0 = h_3 \tag{42}$$

from columns 1, 2, 3, 4, 5, 8 and 1, 2, 3, 4, 5, 9 of (5) respectively, so that

$$a_2 = a_1^2, \qquad a_3 = a_1^3. \tag{43}$$

If $a_1 = 0$, then we have (2); hence we take $a_1 \neq 0$.

4.81. If we have

$$0\,0\,0,\ 0\,0\,1,\ 1\,0\,0,\ 1\,0\,0,$$

then columns 3, 4, 5, 8, 9, 11 and 3, 4, 5, 8, 9, 12 of (5) respectively, give

$$\begin{vmatrix} a_3 & a_4 & a_5 \\ a_2 & a_3 & a_4 \\ 0 & 1 & a_1 \end{vmatrix} = 0, \begin{vmatrix} a_3 & a_4 & a_5 & a_6 \\ a_2 & a_3 & a_4 & a_5 \\ 0 & 1 & a_1 & a_2 \\ 0 & 0 & 1 & a_1 \end{vmatrix} = 0, \text{ so that } \begin{vmatrix} a_3 & a_4 & a_6 \\ a_2 & a_3 & a_5 \\ 0 & 1 & a_2 \end{vmatrix} = 0.$$

Subtract a_1 times row 2 from row 1 and use (43). The first and third determinants give respectively

$$a_2[a_1(a_4 - a_1 a_3) - (a_5 - a_1 a_4)] = 0, \tag{44}$$

$$a_2[a_2(a_4 - a_1 a_3) - (a_6 - a_1 a_5)] = 0. \tag{45}$$

Since $a_2 \neq 0$, (43), (44), (45) give

$$a_1(a_5 - a_1 a_4) = a_6 - a_1 a_5.$$

On using (43), we have $a_1\bar{a}_1 - a_1^2\bar{a}_1^2 = 1 - a_1\bar{a}_1$, and so $a_1\bar{a}_1 = 1$. Then (45) gives $a_4 = a_1^4$ so that $\bar{a}_1^2 = \bar{a}_2 = a_1^4$, $a_5 = a_1^5$, $a_1^6 = 1$, and we have (3 a).

4.82. If we have

$$0\,0\,0,\ 0\,0\,1,\ 1\,0\,0,\ 0\,1\,0 \quad \text{or} \quad 0\,0\,0,\ 0\,0\,1,\ 1\,0\,0,\ 0\,0\,1,$$

then columns 1, 2, 3, 4, 5, 10 of (5) give

$$h_4 = 0.$$

Hence $a_4 = a_1^4$ and, as above, $a_1^6 = 1$ and we have (3 a).

4.9. *Distribution* (*i*). We have

$$a_1 = 0 \quad \text{and} \quad a_3 = a_1 a_2,$$

from columns 1, 2, 3, 4, 5, 7 and 2, 3, 4, 5, 7, 9 of (5) respectively. If the fourth block is 0 1 0 or 0 0 1, then columns 2, 3, 4, 5, 7, 10 of (5) give

$$a_4 = a_2^2,$$

so that $\bar{a}_2 = a_2^2$ and $a_2^3 = 1$, and we have (3 a) as in § 4.52. We consider

$$0\,0\,0,\ 0\,0\,1,\ 0\,1\,0,\ 1\,0\,0.$$

Columns 2, 3, 4, 5, 7, 11 and 2, 3, 4, 5, 7, 12 of (5) give

$$a_2(a_4 - a_2^2) = a_6 - a_2 a_4, \tag{46}$$

by a similar argument to that which gave (44) and (45). Put $a_2 = Re^{i\theta}$ (R, θ real), and (46) gives

$$R^2 - R^3 e^{3i\theta} = 1 - R^2.$$

Hence

$$a_2 = R\omega,$$

where $\omega^3 = 1$, and $R = 1$ or $R^2 = R + 1$.

If $R = 1$, we have (3 a), and, if $R^2 = R + 1$, we have (3 b), as in § 4.31.

4.10. *Distribution* (*j*). We have $a_1 = a_2 = 0$ and as in 4.2 we have (4) or (3 a).

I have to thank Dr. A. J. Macintyre for suggesting this problem and for his advice and encouragement in the preparation of the paper.

JACOBI TRANSFORMS

By E. J. SCOTT (*Urbana, Illinois*)

[Received 27 March 1952]

1. Introduction

By making use of a suitable kernel, integral transforms can be defined which will solve boundary-value problems appropriate to that integral transform with a directness that is lacking in the classical method. Thus, according to the partial differential equation and the boundary conditions a Laplace, complex Fourier, Hankel, or Mellin transform may be used.

Recently C. J. Tranter† considered a Legendre polynomial as a kernel of a finite integral transform which he defined as a Legendre transform and proceeded to show its usefulness in resolving certain boundary value problems. It is the purpose of this paper to introduce a more general transform, of which the Legendre transform is a special case, and thus to extend its utility to a wider class of partial differential equations.

2. Definition and properties of the Jacobi polynomials

The Jacobi polynomial $P_n^{(\alpha,\beta)}(x)$ is defined by means of the expression

$$P_n^{(\alpha,\beta)}(x) = \frac{(-1)^n}{2^n n!}(1-x)^{-\alpha}(1+x)^{-\beta}\frac{d^n}{dx^n}[(1-x)^{\alpha+n}(1+x)^{\beta+n}], \quad (2.1)$$

where α and β are arbitrary real numbers greater than -1 and n is a non-negative integer. When $\alpha = \beta = 0$, this formula reduces to Rodrigues's formula

$$P_n^{(0,0)}(x) = \frac{(-1)^n}{2^n n!}\frac{d^n}{dx^n}[(1-x)^n(1+x)^n],$$

which generates the Legendre polynomials.

It is well known‡ that the Jacobi polynomials are orthogonal over the interval $(-1, 1)$ with respect to the weight function $(1-x)^\alpha(1+x)^\beta$. In fact, for non-negative integers m and n, we have

$$\int_{-1}^{1}(1-x)^\alpha(1+x)^\beta P_m^{(\alpha,\beta)}(x)P_n^{(\alpha,\beta)}(x)\,dx = \begin{cases}0 & (m \neq n),\\ \delta_n & (m = n),\end{cases} \quad (2.2)$$

where

$$\delta_n = \frac{2^{\alpha+\beta+1}\Gamma(\alpha+n+1)\Gamma(\beta+n+1)}{n!\,(\alpha+\beta+2n+1)\Gamma(\alpha+\beta+n+1)}. \quad (2.3)$$

If $n = \alpha+\beta+1 = 0$, then $\delta_0 = \Gamma(\alpha+1)\Gamma(\beta+1)$.

† C. J. Tranter, *Quart. J. of Math.* (Oxford) (2), 1 (1950), 1–8.

‡ G. Szegö, *Orthogonal Polynomials* (American Math. Soc., 1939), Chap. IV.

Furthermore, it can be shown that $P_n^{(\alpha,\beta)}(x)$ satisfies the following differential equation

$$(1-x^2)\frac{d^2}{dx^2}P_n^{(\alpha,\beta)}(x)+[(\beta-\alpha)-(\alpha+\beta+2)x]\frac{d}{dx}P_n^{(\alpha,\beta)}(x)+$$
$$+n(\alpha+\beta+n+1)P_n^{(\alpha,\beta)}(x)=0, \quad (2.4)$$

which for $\alpha=\beta=0$ reduces to the Legendre equation

$$(1-x^2)\frac{d^2P_n(x)}{dx^2}-2x\frac{dP_n(x)}{dx}+n(n+1)P_n(x)=0, \quad (2.5)$$

where $P_n(x)\equiv P_n^{(0,0)}(x)$.

If, in (2.4), α and β are replaced by the common positive integer m, and n is replaced by $n-m$, then (2.4) becomes

$$(1-x^2)\frac{d^2}{dx^2}P_{n-m}^{(m,m)}(x)-2(m+1)x\frac{d}{dx}P_{n-m}^{(m,m)}(x)+$$
$$+(n-m)(n+m+1)P_{n-m}^{(m,m)}(x)=0,$$

and any polynomial solution of this equation is a multiple of the mth derivative of $P_n(x)$, i.e. $P_n^{(m)}(x)$. It follows that the derivatives of the Legendre polynomials are but particular cases of the Jacobi polynomials. The connexion between the Jacobi polynomials and the derivatives of the Legendre polynomials is given by the formula

$$P_n^{(m)}(x)=\frac{(n+m)!}{2^m n!}P_{n-m}^{(m,m)}(x),$$

where $m\leqslant n$.

Also of use to us in the sequel will be the values

$$P_n^{(\alpha,\beta)}(1)=\frac{\Gamma(n+\alpha+1)}{n!\,\Gamma(\alpha+1)}, \qquad P_n^{(\alpha,\beta)}(-1)=(-1)^n\frac{\Gamma(n+\beta+1)}{n!\,\Gamma(\beta+1)}.$$

3. Definition of the finite Jacobi transform and its inversion formula

If a function $F(x)$ defined on the interval $(-1,1)$ is multiplied by $P_n^{(\alpha,\beta)}(x)$ and integrated with respect to x over this interval, then the resulting function, which I shall denote by $f^{(\alpha,\beta)}(n)$, will be called the *Jacobi transform* of $F(x)$: symbolically,

$$J\{F(x)\}=f^{(\alpha,\beta)}(n)=\int_{-1}^{1}F(x)P_n^{(\alpha,\beta)}(x)\,dx. \quad (3.1)$$

Let us now suppose that $F(x)$ admits of the following expansion

$$F(x)=\sum_{n=0}^{\infty}c_n(1-x)^{\alpha}(1+x)^{\beta}P_n^{(\alpha,\beta)}(x). \quad (3.2)$$

Then because of formulae (2.2) the coefficients c_n are given by

$$c_n = \frac{1}{\delta_n} \int_{-1}^{1} F(x) P_n^{(\alpha,\beta)}(x)\, dx = \frac{1}{\delta_n} f^{(\alpha,\beta)}(n), \tag{3.3}$$

where δ_n is defined in (2.3). Inserting this value of c_n in (3.1), we see that the inversion formula corresponding to (3.1) is

$$F(x) = \sum_{n=0}^{\infty} \frac{1}{\delta_n} f^{(\alpha,\beta)}(n)(1-x)^{\alpha}(1+x)^{\beta} P_n^{(\alpha,\beta)}(x). \tag{3.4}$$

Formulae (3.1) and (3.4) are basic for the solution of certain partial differential equations.

4. The group of terms excluded from a partial differential equation by the Jacobi transform

The Jacobi transform is useful in excluding the following group of terms from a differential equation, namely,

$$\partial/\partial x\{(1-x^2)\partial U(x,t)/\partial x\} + [(\alpha-\beta)+(\alpha+\beta)x]\,\partial U(x,t)/\partial x, \tag{4.1}$$

where $\alpha > -1, \beta > -1$. For I shall show that

$$J_x\{\partial/\partial x[(1-x^2)\,\partial U(x,t)/\partial x] + [(\alpha-\beta)+(\alpha+\beta)x]\,\partial U(x,t)/\partial x\}$$
$$= -(n+1)(n+\alpha+\beta)u^{(\alpha,\beta)}(n,t) + [\{(\alpha-\beta)+(\alpha+\beta)x\}P_n^{(\alpha,\beta)}(x)U(x,t)]_{-1}^{1}, \tag{4.2}$$

where the subscript x implies that the transform is being taken with respect to x and

$$J_x\{U(x,t)\} = u^{(\alpha,\beta)}(n,t). \tag{4.3}$$

The Jacobi transform of (4.1) with respect to x is by definition

$$\int_{-1}^{1} \partial/\partial x\{(1-x^2)\,\partial U/\partial x\} P_n^{(\alpha,\beta)}(x)\, dx + \int_{-1}^{1} [(\alpha-\beta)+(\alpha+\beta)x]\,\partial U/\partial x\; P_n^{(\alpha,\beta)}(x)\, dx. \tag{4.4}$$

Integrating the first term of (4.4) by parts twice and making use of the fact that $P_n^{(\alpha,\beta)}(x)$ satisfies the differential equation (2.4), which can be written

$$\frac{d}{dx}\left\{(1-x^2)\frac{dP_n^{(\alpha,\beta)}(x)}{dx}\right\}$$
$$= -[(\beta-\alpha)-(\alpha+\beta)x]\frac{dP_n^{(\alpha,\beta)}(x)}{dx} - n(\alpha+\beta+n+1)P_n^{(\alpha,\beta)}(x),$$

we find easily that

$$\int_{-1}^{1} \partial/\partial x\{(1-x^2)\,\partial U/\partial x\}P_n^{(\alpha,\beta)}(x)\,dx$$

$$= \int_{-1}^{1} U[(\alpha-\beta)+(\alpha+\beta)x]\frac{dP_n^{(\alpha,\beta)}(x)}{dx}\,dx - n(\alpha+\beta+n+1)\int_{-1}^{1} UP_n^{(\alpha,\beta)}(x)\,dx. \tag{4.5}$$

The second term of (4.4) when integrated by parts once yields

$$\int_{-1}^{1} [(\alpha-\beta)+(\alpha+\beta)x]\,\partial U/\partial x\; P_n^{(\alpha,\beta)}(x)\,dx$$

$$= [\{(\alpha-\beta)+(\alpha+\beta)x\}P_n^{(\alpha,\beta)}(x)\,U(x,t)]_{-1}^{1} -$$

$$-(\alpha+\beta)\int_{-1}^{1} UP_n^{(\alpha,\beta)}(x)\,dx - \int_{-1}^{1} U[(\alpha-\beta)+(\alpha+\beta)x]\frac{dP_n^{(\alpha,\beta)}(x)}{dx}\,dx. \tag{4.6}$$

Adding expressions (4.5) and (4.6) we obtain (4.2).

5. An application of the Jacobi transform

The heat equation for one-dimensional flow is given by

$$\frac{\partial}{\partial x}\left(K\frac{\partial U(x,t)}{\partial x}\right) + P(x,t) = \rho c\frac{\partial U(x,t)}{\partial t}, \tag{5.1}$$

where ρ is the density of the solid, c is the specific heat, both assumed constant, K is the thermal conductivity, $P(x,t)$ is a continuous source of heat within the solid, and $U(x,t)$ is the temperature of the solid at x at time t. If the thermal conductivity K is proportional to $(1-x^2)$ and the source $P(x,t)$ is a linear function $(a+bx)$ times $\partial U(x,t)/\partial x$, where a, b and the constant of proportionality d are real numbers, then (5.1) assumes the form

$$\frac{\partial}{\partial x}\left[(1-x^2)\frac{\partial U(x,t)}{\partial x}\right] + \frac{a+bx}{d}\frac{\partial U(x,t)}{\partial x} = \frac{\rho c}{d}\frac{\partial U(x,t)}{\partial t}, \tag{5.2}$$

the left-hand side of which lends itself to simplification by applying to it the Jacobi transform provided that $(a+b)/d > -2$ and $(b-a)/d > -2$. These conditions on a and b must be imposed in order that $\alpha > -1$ and $\beta > -1$.

Consider now a non-homogeneous bar with ends at $x = -1$ and $x = 1$ whose lateral surface is insulated. Since the thermal conductivity $K = d(1-x^2)$ vanishes at $x = 1$ and $x = -1$, it follows that the ends are also insulated. Suppose that initially

$$U(x,0) = F(x) \quad (-1 < x < 1) \tag{5.3}$$

and that at the ends

$$U(1,t) = \phi(t) \quad \text{and} \quad U(-1,t) = \psi(t) \quad (t > 0). \tag{5.4}$$

Taking the Jacobi transforms of equations (5.2) and (5.3) with respect to x, we obtain

$$\frac{\rho c}{d}\frac{d}{dt}u^{(\alpha,\beta)}(n,t)+(n+1)\left(n+\frac{b}{d}\right)u^{(\alpha,\beta)}(n,t)$$

$$= \frac{a+b}{d}P_n^{(\alpha,\beta)}(1)\phi(t)+\frac{b-a}{d}P_n^{(\alpha,\beta)}(-1)\psi(t), \tag{5.5}$$

where $$\alpha = \frac{a+b}{2d}, \qquad \beta = \frac{b-a}{2d},$$

and $$u(n,0) = \int_{-1}^{1} F(x)P_n^{(\alpha,\beta)}(x)\,dx. \tag{5.6}$$

Solving (5.5) and making use of (5.6) we readily find that

$$u^{(\alpha,\beta)}(n,t) = \frac{a+b}{\rho d}P_n^{(\alpha,\beta)}(1)e^{-(n+1)\{(nd+b)/\rho c\}t}\int_0^t \phi(\tau)e^{(n+1)\{(nd+b)/\rho c\}\tau}\,d\tau+$$

$$+\frac{b-a}{\rho c}P_n^{(\alpha,\beta)}(-1)e^{-(n+1)\{(nd+b)/\rho c\}t}\int_0^t \psi(\tau)e^{(n+1)\{(nd+b)/\rho c\}\tau}\,d\tau+$$

$$+e^{-(n+1)\{(nd+b)/\rho c\}t}\int_{-1}^{1} F(x)P_n^{(\alpha,\beta)}(x)\,dx. \tag{5.7}$$

Therefore, by the inversion formula (3.4),

$$U(x,t)$$

$$= \sum_{n=0}^{\infty}\frac{1}{\delta_n}(1-x)^{(a+b)/2d}(1+x)^{(b-a)/2d}P_n^{\{(a+b)/2d,(b-a)/2d\}}(x)u^{\{(a+b)/2d,(b-a)/2d\}}(n,t). \tag{5.8}$$

The analysis given above, although formal, can be made rigorous by showing that the solution satisfies the differential equation and the boundary conditions.

MANIFOLDS WHOSE POINTS IMAGE PAIRS OR TRIOS OF POINTS CHOSEN FROM THE GROUPS OF A LINEAR SERIES

By J. G. BRENNAN (*Swansea*)

[Received 9 April 1952]

1. Introduction

V. C. MORTON (3) has considered what is, in effect, a linear series g_n^{p-1} on a rational normal curve C in $[r]$. The osculating primes of C at any $r > p-1$ points all chosen from the same group G of g_n^{p-1} intersect in a point P, and it is shown that as G varies in g_n^{p-1}, P describes a variety V of dimension $p-1$ and order $\binom{n-p+1}{r-p+1}$ the points of which may be regarded as imaging the groups of r points chosen from groups of g_n^{p-1}. This suggests the problem of investigating those manifolds whose points image the groups of k points contained in a linear series g_n^r on a curve of general genus. The problem will be significant provided that

$$r < k \leqslant n.$$

I denote such a manifold by $V_r(k, n)$, the series g_n^r being given on a curve of genus p in $[k]$. This paper is concerned with curves $V_1(2, n)$ and surfaces $V_2(3, n)$. The investigation involves the consideration of special cases of a further problem which may be stated as follows: *Given three linear series*† $g_{n_1}^{r_1}$, $g_{n_2}^{r_2}$, $g_{n_3}^{r_3}$ *on the same curve, how many trios of groups* G_1, G_2, G_3 *are there, one from each series, such that* G_1, G_2, G_3 *have* k_{123} *points in common while* G_i *and* G_j *have a further* k_{ij} *points in common, where* $i, j = 1, 2, 3$? There will be a finite number of such trios provided that

$$k_{12}+k_{13}+k_{23}+2k_{123} = r_1+r_2+r_3.$$

I then denote the number in question by $N\begin{bmatrix} r_1, & r_2, & r_3 \\ n_1, & n_2, & n_3 \end{bmatrix}; k_{12}, k_{13}, k_{23}; k_{123}\Big]$. In the cases considered here, $k_{12} = 0$, and, where there is no risk of ambiguity, this number will be written, for short, as $N[k_{13}, k_{23}; k_{123}]$.

1.1. *The genus and order of* $V_1(k, n)$. Let there be given a g_n^1 on a curve C of genus p in $[k]$, let $P_1, P_2, \ldots, P_k$ be k points from the same group G of g_n^1, and let the osculating primes of C at these points intersect in $T_{1,2,\ldots,k}$. We require the genus p' of the locus $V_1(k, n)$ of T as G varies in g_n^1.

† Here, and hereafter, the linear series concerned are *general* series.

Quart. J. Math. Oxford (2), 4 (1953), 41–53.

Clearly C and V_1 are related in a correspondence with indices

$$\left[k, \binom{n-1}{k-1}\right].$$

Let z and z' be the numbers of branch-points of this correspondence on C and V_1 respectively. Now, if P_1 is a branch-point, then two of the $n-1$ remaining points of G must coincide; so the number of branch-point *positions* on C is $(n-2)[2(n-1)+2p]$. Let P_2 and P_3 be the coincident points in such a group G. Then the points $T_{1,2,4,\ldots,(k+1)}$ and $T_{1,3,4,\ldots,(k+1)}$ coincide on V_1, and this holds for each choice of $k-2$ points from G apart from P_1 and either P_2 or P_3. Hence to each branch-point such as P_1 correspond $\binom{n-3}{k-2}$ different coincidences on V_1, and

$$z = (n-2)\binom{n-3}{k-2}[2(n-1)+2p].$$

Again, two of the points $P_1, P_2, \ldots, P_k$ corresponding to a given T can coincide only if T lies on the osculating $[k-2]$ to C at this coincidence. Thus the branch-points on V_1 are the points of intersection of this $[k-2]$ with the $k-2$ osculating primes at any $k-2$ points chosen from the remaining $n-2$ points of the group. Hence

$$z' = \binom{n-2}{k-2}[2(n-1)+2p].$$

Finally, from Zeuthen's formula

$$\alpha'(2p-2)+z = \alpha(2p'-2)+z'$$

with $\alpha = k$ and $\alpha' = \binom{n-1}{k-1}$ we find†

$$p' = 1+\frac{(n-2)(n-3)\ldots(n-k)}{(k-1)!}p+\frac{(n-1)(n-2)\ldots(n-k+1)[(k-1)n-k^2]}{k!}.$$

It is interesting to note that (i) if $k = n$, then $p' = 0$; (ii) if k and $n-k$ be interchanged in the expression for p', the result is unaltered. This is to be expected since (i) complete groups of g_n^1 form a rational totality and (ii) the groups of k points are in $(1, 1)$ correspondence with the groups of $n-k$ points.

Let C be of class m, and consider the group of m points of osculation of the osculating primes of C through a point P of a general prime π. As P varies in π, the corresponding group varies in a g_m^{k-1}. Each intersection of $V_1(k, n)$ with π gives rise to a group of k points on C which are

† I am indebted to Professor Morton for this result.

common to both g_n^1 and g_m^{k-1}. Hence the order of $V_1(k,n)$ is the number of groups of k points (or k-ads) common to g_n^1 and g_m^{k-1}. This number is known (**4**) to be

$$m\binom{n-1}{k-1}-\binom{n-2}{k-2}(n+p-1).$$

1.2. *The multiple points of* $V_1(2,n)$. These arise in two ways. Consider the g_m^2 of points of contact of tangents to C from all points of the plane. Then (i) there will be a finite number of groups of g_m^2 each containing two pairs of points, one pair belonging to one group of g_n^1 and the other to a different group of g_n^1, and (ii) there will be a finite number of groups of g_m^2 each having three points in common with a group of g_n^1. Each configuration (i) gives rise to a double point on $V_1(2,n)$ and each configuration (ii) to a triple point.

Let the number arising under (i) be Z. Any pair of points from a group G of g_n^1 determines a group $\bar{G}$ of g_m^2, and the $m-2$ remaining points of $\bar{G}$ then vary in an algebraic series γ_{m-2}^1 of index ν with d double points. The number of pairs of points common to γ_{m-2}^1 and g_n^1 is then (**4**)

$$2Z = n\nu(m-3)-\tfrac{1}{2}d,$$

where ν is the number of common pairs of points of g_{m-1}^1 and g_n^1,

i.e. $$\nu = (m-2)(n-1)-p.$$

The $m-2$ remaining points of those groups of g_m^2 with a double point form a series $\bar{\gamma}_{m-2}^1$ of index $\bar{\nu}$, where $\bar{\nu}$ is the number of double points of a g_{m-1}^1, and with $\bar{d}$ double points, where $\bar{d}$ is twice the number of groups of g_m^2 with two double points. Now d is the number of common pairs of $\bar{\gamma}_{m-2}^1$ and g_n^1. It follows that

$$Z = \tfrac{1}{2}(m-2)(m-3)(n-1)^2-(m-3)(n-1)p+\tfrac{1}{2}p(p-1).$$

The number of triple points of $V_1(2,n)$ is at once seen to be

$$\tfrac{1}{2}(m-2)(n-1)(n-2)-p(n-2).$$

Counting each triple point as equivalent to three double points, it may be verified that the total number of multiple points thus obtained is the correct number for a curve of order $(m-1)(n-1)-p$ and genus $\tfrac{1}{2}(n-2)(n-3)+p(n-2)$.

1.3. *The intersections of* $V_1(2,n_1)$ *and* $V_1(2,n_2)$. Given, on the same curve C, two linear series $g_{n_1}^1$ and $g_{n_2}^1$, we now investigate the intersections of the corresponding curves $V_1(2,n_1)$ and $V_1(2,n_2)$. Such intersections arise as follows:

(i) from groups of the series g^2_m containing two pairs of points, the pairs having no common point, one pair belonging to a group of $g^1_{n_1}$, the other to a group of $g^1_{n_2}$;

(ii) from groups of g^2_m containing a pair of points from each of $g^1_{n_1}$, $g^1_{n_2}$, these pairs having a point in common;

(iii) from the common pairs of $g^1_{n_1}$ and $g^1_{n_2}$.

We now find the numbers of intersections arising under these headings.

(i) Consider the γ^1_{m-2} formed by the $m-2$ remaining points of those groups of g^2_m which have a pair of points in common with $g^1_{n_1}$. If ν and d be respectively the index and number of double points of γ^1_{m-2}, then the number required is the number of common pairs of γ^1_{m-2} and $g^1_{n_2}$: that is

$$N\begin{bmatrix} 1 & 1 & 2 \\ n_1, & n_2, & m \end{bmatrix}; 0, 2, 2; 0 = n_2\nu(m-3)-\tfrac{1}{2}d$$

$$= (m-2)(m-3)(n_1-1)(n_2-1)-p(m-3)(n_1+n_2-2)+p(p-1).$$

(ii) Let P be any point of the group of $g^1_{n_1}$ defined by a general point Q of C and let R be any point, other than P or Q, of the group of g^2_m defined by P and Q. This defines a correspondence (Q, R) with indices

$$\{2[(n_1-1)(m-2)-p],\ (n_1-1)(m-2)\}$$

of valency n_1-2. Again $g^1_{n_2}$ generates an elementary correspondence (Q, R') with indices n_2-1. The number required is the number of common corresponding pairs of (Q, R) and (Q, R'), i.e.

$$N\begin{bmatrix} 1 & 1 & 2 \\ n_1, & n_2, & m \end{bmatrix}; 0, 1, 1; 1 = 3(m-2)(n_1-1)(n_2-1)-2p(n_1+n_2-3).$$

(iii) We have at once

$$N\begin{bmatrix} 1 & 1 & 2 \\ n_1, & n_2, & m \end{bmatrix}; 0, 0, 0; 2 = (n_1-1)(n_2-1)-p.$$

Since $V_1(2, n)$ is of order $(m-1)(n-1)-p$, we should have

$$N[2, 2; 0]+N[1, 1; 1]+N[0, 0; 2]$$

$$= [(m-1)(n_1-1)-p][(m-1)(n_2-1)-p],$$

which is true.

2. A particular series γ^1_3 and the correspondence generated by it

The groups of three points common to two series $g^2_{n_1}$ and $g^2_{n_2}$ form a γ^1_3 of index

$$\nu_3 = (n_1-2)(n_2-2)-p$$

with, say, δ_3 double points. Now the number of trios common to $g^2_{n_1}$, $g^2_{n_2}$, and to a third series $g^2_{n_3}$ is known (**2**) to be

$$N\begin{bmatrix}2, & 2, & 2\\ n_1, & n_2, & n_3\end{bmatrix}; 0, 0, 0; 3\Big] = (n_1-2)(n_2-2)(n_3-2)-p(n_1+n_2+n_3)+8p$$

$$= n_3\nu_3-\tfrac{1}{2}\delta_3.$$

Hence $$\delta_3 = 4(n_1-2)(n_2-2)+2p(n_1+n_2-8).$$

Consider the correspondence which relates to a point P all the points of the groups of γ^1_3 through P. This is a correspondence with indices $(2\nu_3, 2\nu_3)$, and of valency γ say,† the united points of which are the double points of γ^1_3. By the Cayley–Brill theorem

$$\delta_3 = 4\nu_3+2\gamma p.$$

Hence $$\gamma = n_1+n_2-6.$$

2.1. *Surfaces $V_2(3, n)$: the intersection of $V_2(3, n_1)$ and $V_2(3, n_2)$.* Given a g^2_n on a space curve C, the locus of the intersection of the osculating planes at any three points of a group is a surface $V_2(3, n)$ whose order is the number of trios common to the given series and to the g^1_m of points of osculation of osculating planes through a variable point of a general line, where m is the class of the carrier curve of g^2_n. Hence $V_2(3, n)$ is of order

$$\tfrac{1}{2}(m-1)(m-2)(n-2)-(m-2)p.$$

Given on C a $g^2_{n_1}$ and a $g^2_{n_2}$, the complete intersection of the surfaces $V_2(3, n_1)$ and $V_2(3, n_2)$ consists of four curves C_0, C_1, C_2, C_3; for to the points of a general plane correspond the groups of a g^2_m on C, and the respective orders of these curves are given by $N\begin{bmatrix}2, & 2, & 2\\ n_1, & n_2, & m\end{bmatrix}; 0, i, j; k\Big]$, where $[i, j; k]$ denotes $[3, 3; 0]$, $[2, 2; 1]$, $[1, 1; 2]$, or $[0, 0; 3]$. From § 2 we have at once

$$N[0, 0; 3] = (m-2)(n_1-2)(n_2-2)-p(m+n_1+n_2-8).$$

2.2. *Calculation of $N[3, 3; 0]$.* Consider the ∞^1 groups of g^2_m which have three points in common with $g^2_{n_1}$. The remaining $m-3$ points in such groups vary in a series $\bar{\gamma}^1_{m-3}$ of index $\bar{\nu}_3$ with $\bar{\delta}_3$ double points, and $N[3, 3; 0]$ is the number of groups of $\bar{\gamma}^1_{m-3}$ which have a trio of points in common with $g^2_{n_2}$. Hence

$$N[3, 3; 0] = n_2\bar{\nu}_3\binom{m-4}{2}-\tfrac{1}{2}(m-5)\bar{\delta}_3.$$

Now $\bar{\nu}_3$ is the number of trios common to a g^1_{m-1} and a $g^2_{n_1}$; hence

$$\bar{\nu}_3 = \tfrac{1}{2}n_1(m-2)(m-3)-(m-3)(m+p-2).$$

† It is easy to show that this correspondence is representable by a single equation. It must therefore be a correspondence with valency.

The remaining $m-2$ points of those groups of g_m^2 with a double point form a γ_{m-2}^1 of index ν', with δ' double points; δ_3 is the number of groups of γ_{m-2}^1 having a trio in common with $g_{n_1}^2$. Hence

$$\delta_3 = n_1\nu'\binom{m-3}{2} - \tfrac{1}{2}(m-4)\delta',$$

where ν' is the number of double points of a g_{m-1}^1 and δ' is twice the number of groups of g_m^2 with two double points (**5**). Hence

$$\nu' = 2(m+p-2) \quad \text{and} \quad \delta' = 4(m+p-2)(m+p-3)-8p,$$

and finally

$$N[3,3;0] = \tfrac{1}{4}(m-2)(m-3)(m-4)(m-5)(n_1-2)(n_2-2)-$$
$$-\tfrac{1}{2}(m-3)(m-4)(m-5)(n_1+n_2-4)p+(m-4)(m-5)p(p-1).$$

2.3. *Calculation of* $N[2,2;1]$. The common trios of $g_{n_1}^2$ and g_m^2 form a γ_3^1 of index $\nu_3 = (n_1-2)(m-2)-p$ with

$$\delta_3 = 4(n_1-2)(m-2)+2p(n_1+m-8)$$

double points. If the points of those trios through a point P (other than P itself) be points Q, we have a correspondence $\overline{T}_1$: (P,Q) with indices $(2\nu_3, 2\nu_3)$ [cf. § 2]. If the remainders of these trios with respect to g_m^2 be points R, these points vary in the $\bar{\gamma}_{m-3}^1$ of § 2.2 and we have a correspondence $\overline{T}_2$: (P,R) with indices $[3\bar{\nu}_3, \nu_3(m-3)]$. When P is given, there are determined ν_3 groups of $\bar{\gamma}_{m-3}^1$. Any two points from the same group of $\bar{\gamma}_{m-3}^1$ determine a group of $g_{n_2}^2$. If the further points thus obtained be points S, we have a correspondence $\overline{T}_3$: (P,S) with indices

$$\left[3\alpha, \nu_3\binom{m-3}{2}(n_2-2)\right],$$

where α is the number of pairs common to $g_{n_2-1}^1$ and $\bar{\gamma}_{m-3}^1$, i.e.

$$\alpha = (n_2-1)\bar{\nu}_3(m-4)-\tfrac{1}{2}\delta_3.$$

$\overline{T}_1+\overline{T}_2$ is of valency ν_3 and $(m-4)\overline{T}_2+\overline{T}_3$ is of valency zero. Since $\overline{T}_1$ is of valency n_1+m-6 [§ 2], it follows that $\overline{T}_3$ has valency $(m-4)(\gamma-\nu_3)$. The number of united points of $\overline{T}_3$ is the number required, and by the Cayley–Brill formula

$$N[2,2;1] = 3\alpha+\nu_3\binom{m-3}{2}(n_2-2)+2(m-4)(\gamma-\nu_3)p$$
$$= 2(m-2)(m-3)(m-4)(n_1-2)(n_2-2)-$$
$$-\tfrac{1}{2}(m-3)(m-4)[7(n_1+n_2)-32]p+5(m-4)p(p-1).$$

2.4. *Calculation of* $N[1,1;2]$. With the notation of §§ 2.2, 2.3 I shall call a group of γ_3^1 and a group of $\bar{\gamma}_{m-3}^1$ a pair of *complementary* groups if together they form a group of g_m^2. Let R be a general point of C. The groups of $g_{n_2}^2$ through R form a $g_{n_2-1}^1$ which has β pairs of points Q_i and Q_i' $(i = 1, 2, \ldots, \beta)$ in common with γ_3^1, where

$$\beta = 2(n_2-1)\nu_3 - \tfrac{1}{2}\delta_3.$$

The β complementary groups from $\bar{\gamma}_{m-3}^1$ then furnish $\beta(m-3)$ points S. Thus we have a correspondence $\overline{T}_1'$: (R, S) with indices

$$[3\bar{\nu}_3(n_2-2), \beta(m-3)].$$

The number of united points of $\overline{T}_1'$ is the number required.

If P_i be the third point of that group of γ_3^1 containing Q_i and Q_i', we have also the correspondences $\overline{T}_2'$: (R, P) with indices $[\nu_3(n_2-2), \beta]$ and $\overline{T}_3'$: (R, Q) with indices $[2\nu_3(n_2-2), 2\beta]$.

$\overline{T}_1' + \overline{T}_2' + \overline{T}_3'$ is of valency zero, and, if U_1, U_2, U_3 be the numbers of united points of $\overline{T}_1'$, $\overline{T}_2'$, $\overline{T}_3'$, then

$$U_1 + U_2 + U_3 = 3\bar{\nu}_3(n_2-2) + \beta(m-3) + 3\nu_3(n_2-2) + 3\beta,$$

where $U_1 = N[1,1;2]$ and $U_2 = 3N[0,0;3]$. U_3 is the number of groups of γ_3^1 containing points Q and Q', where Q is an ordinary point of a group of $g_{n_2}^2$ while Q' is a double point of the same group. Now Q' and Q correspond *via* γ_3^1 in a correspondence $(2\nu_3, 2\nu_3)$ of valency n_1+m-6, while, if Q' is a double point of $g_{n_2}^2$ and Q an ordinary point of the same group, then Q' and Q also correspond in a correspondence with indices $[2(n_2+p-2),\ n_2-2]$ of valency 2. U_3 is the number of common corresponding pairs of the last two correspondences, so that

$$U_3 = 2[(n_1-2)(m-2)-p][3n_2+2p-6] - 4p(n_1+m-6).$$

We thus find

$$N[1,1;2] = \tfrac{7}{2}(m-2)(m-3)(n_1-2)(n_2-2) - \\ -(m-3)[5(n_1+n_2)+m-28]p + 4p(p-1).$$

Since the order of $V_2(3, n)$ is $\frac{1}{2}(m-1)(m-2)(n-2) - (m-2)p$, we have, as a check, the identity

$$N[3,3;0] + N[2,2;1] + N[1,1;2] + N[0,0;3] \\ = [\tfrac{1}{2}(m-1)(m-2)(n_1-2) - (m-2)p][\tfrac{1}{2}(m-1)(m-2)(n_2-2) - (m-2)p].$$

3. Multiple points and multiple curves on $V_2(3, n)$

(i) By the usual construction, to all the points of $[3]$ corresponds on C a g_m^3. A series g_n^2 on C will have in common with g_m^3 a number (**1**)

$$\tfrac{1}{12}(m-3)(m-4)(n-2)(n-3)(n-4) - \\ -\tfrac{1}{2}(m-4)(n-3)(n-4)p + \tfrac{1}{2}(n-4)p(p-1)$$

of 5-ads, each of which gives rise to a point of multiplicity $\binom{5}{3} = 10$ on $V_2(3, n)$.

(ii) There are ∞^1 groups of g^3_m each containing two trios of points (with no common point) each trio from a different group of g^2_n. These groups give rise to a double curve D_0 on V_2. Again there are ∞^1 groups of g^3_m containing 5 points, say P_1, P_2, R, Q_1, Q_2, where P_1, P_2, R belong to one group of g^2_n and R, Q_1, Q_2 to another group of g^2_n. Such groups give rise to a double curve D_1 on V_2. The orders of D_0 and D_1 may be denoted formally by

$$\tfrac{1}{2}N\begin{bmatrix} 2, & 2, & 2 \\ n, & n, & m \end{bmatrix}; 0, 3, 3; 0 \quad \text{and} \quad \tfrac{1}{2}N\begin{bmatrix} 2, & 2, & 2 \\ n, & n, & m \end{bmatrix}; 0, 2, 2; 1 :$$

that is

$$\tfrac{1}{8}(m-2)(m-3)(m-4)(m-5)(n-2)^2 - \\ -\tfrac{1}{2}(m-3)(m-4)(m-5)(n-2)p + \tfrac{1}{2}(m-4)(m-5)p(p-1)$$

and

$$(m-2)(m-3)(m-4)(n-2)^2 - \tfrac{1}{2}(m-3)(m-4)(7n-16)p + \\ + \tfrac{5}{2}(m-4)p(p-1)$$

respectively. Though the matter will not be pursued further here, it may be remarked that there are triple points on D_0 and D_1 which are triple also for V_2. On D_0 such points arise from groups of g^3_m containing three trios of points, each trio from a different group of g^2_n. On D_1 triple points arise from groups of g^3_m containing points $P_1, P_2, Q_1, Q_2, R_1, R_2, S$ where each of the trios $P_1 P_2 S$, $Q_1 Q_2 S$, $R_1 R_2 S$ belongs to a different group of g^2_n.

(iii) The common 4-ads of g^2_n and g^3_m form a γ^1_4, each group of which gives rise to one point of a quadruple curve Q on V_2. The order of Q is the number of common 4-ads of g^2_n and the g^2_m corresponding to a general plane π, each such 4-ad corresponding to a quadruple point on the curve of section of V_2 by π: that is (1)

$$\tfrac{1}{4}(m-2)(m-3)(n-2)(n-3) - (m-3)(n-3)p + \tfrac{1}{2}p(p-1).$$

3.1. *The intersections of $V_2(3, n_1)$ and Q_2.* I denote the quadruple curves on the surfaces $V_2(3, n_1)$ and $V_2(3, n_2)$ of § 2.1 by Q_1 and Q_2 respectively, and proceed to examine the intersections of $V_2(3, n_1)$ and Q_2 since such an examination yields information about the curves C_0, C_1, C_2, C_3. The intersections in question arise in four ways and the corresponding numbers of intersections may be written $N\begin{bmatrix} 2, & 2, & 3 \\ n_1, & n_2, & m \end{bmatrix}; 0, i, j; k\Big]$ where $[i, j; k]$ denotes $[3, 4; 0]$, $[2, 3; 1]$, $[1, 2; 2]$, or $[0, 1; 3]$. Now $[3, 4; 0]$ may

be regarded as arising from a configuration $[3,3;0]$ in four different ways; $[2,3;1]$ arises from $[2,2;1]$ in three ways and from $[3,3;0]$ in one way; $[1,2;2]$ arises from $[1,1;2]$ in two ways and from $[2,2;1]$ in two ways; while $[0,1;3]$ arises from $[1,1;2]$ in three ways and from $[0,0;3]$ in one way. Hence, at each intersection $[3,4;0]$, C_0 has a quadruple point; at each intersection $[2,3;1]$, C_1 has a triple point through which passes one branch of C_0; at each intersection $[1,2;2]$, both C_1 and C_2 have double points; while, at each intersection $[0,1;3]$, C_2 has a triple point through which passes one branch of C_3.

3.2. *Calculation of* $N[3,4;0]$. The groups of $m-3$ remaining points from those groups of g^3_m which have a trio in common with $g^2_{n_1}$ form a γ^2_{m-3} of index

$$\nu = \tfrac{1}{2}(n_1-2)(m-3)(m-4)-p(m-4).$$

Let d_1, d_{11}, d_2 denote respectively the number of double points of the γ^1_{m-4} defined within γ^2_{m-3} by a general point of C, the number of groups of γ^2_{m-3} with two double points, and the number of triple points of γ^2_{m-3}. Then (6)

$$N[3,4;0] = \nu\binom{n_2}{2}\binom{m-5}{2}+(m-6)(\tfrac{1}{3}d_2-\tfrac{1}{2}n_2 d_1)+\tfrac{1}{4}d_{11},$$

this being the number of 4-ads common to γ^2_{m-3} and $g^2_{n_2}$.

The groups of g^3_m through a point Q form a g^2_{m-1}; d_1 is the number of groups of g^2_{m-1} which have a double point and which have a trio in common with $g^2_{n_1}$. Select a double point Q'; then, as Q' varies (Q remaining fixed), the remaining $m-3$ points vary in a series $\bar{\gamma}^1_{m-3}$, so that d_1 is the number of trios common to $g^2_{n_1}$ and $\bar{\gamma}^1_{m-3}$. The latter series has index $\bar{\nu}$ and has $\bar{\delta}$ double points, where

$$\bar{\nu} = 2(m+p-3) \quad \text{and} \quad \bar{\delta} = 4(m+p-3)(m+p-4)-8p.$$

Then

$$d_1 = n_1\bar{\nu}\binom{m-4}{2}-\tfrac{1}{2}(m-5)\,\bar{\delta}.$$

Again, d_{11} is the number of groups of g^3_m which have two double points and also a trio in common with $g^2_{n_1}$. On removing the two double points from the groups of g^3_m containing them we have a γ^{*1}_{m-4} of index ν^* and with δ^* double points, where ν^* is the number of groups of g^2_{m-1} with two double points and δ^* is three times the number of groups of g^3_m with three double points. Thus $\nu^* = \tfrac{1}{2}\bar{\delta}$ and (5)

$$\delta^* = 4[(m-3)(m-4)(m-5)+3(m-4)(m-5)p+ \\ +3(m-5)p(p-1)+p(p-1)(p-2)]$$

and

$$d_{11} = n_1\nu^*\binom{m-5}{2}-\tfrac{1}{2}(m-6)\,\delta^*.$$

Finally, d_2 is the number of common trios of $g^2_{n_1}$ and the series $\bar{\gamma}^1_{m-3}$ formed by the groups of $m-3$ remaining points from those groups of g^3_m with a triple point, which series has index $\bar{\nu}$ and $\bar{\delta}$ double points where $\bar{\nu}$ is the number of triple points of a g^2_{m-1} and $\bar{\delta}$ is the number of groups of g^3_m with a double point and a triple point (**5**). Hence

$$\bar{\nu} = 3(m+2p-3), \qquad \bar{\delta} = 6[(m-3)(m-4)+3p(m-4)+2p(p-1)]$$

and

$$d_2 = n_1\bar{\nu}\binom{m-4}{2} - \tfrac{1}{2}(m-5)\,\bar{\delta}.$$

We arrive ultimately at the result

$$N[3,4;0] = \tfrac{1}{8}(m-3)(m-4)(m-5)(m-6)(n_1-2)(n_2-2)(n_2-3) -$$
$$-\tfrac{1}{4}(m-4)(m-5)(m-6)[2(n_1-2)+(n_2-2)](n_2-3)p+$$
$$+\tfrac{1}{4}(m-5)(m-6)[n_1-2+4(n_2-3)]p(p-1)-\tfrac{1}{2}(m-6)p(p-1)(p-2).$$

3.3. *Calculation of* $N[0,1;3]$. The groups of $g^2_{n_2}$ through a point P form a $g^1_{n_2-1}$ which has ν trios of points R in common with $g^2_{n_1}$, where

$$\nu = \tfrac{1}{2}(n_1-2)(n_2-2)(n_2-3)-p(n_2-3).$$

Each such trio defines a group of g^3_m. Let the points of such groups, other than the points of the trios, be points Q. Then we have a correspondence $\bar{T}_1$: (P,Q) with indices $[\alpha(n_2-3), \nu(m-3)]$ where α is the number of trios common to $g^2_{n_1}$, $g^2_{n_2}$ and to the g^2_{m-1} formed by the groups of g^3_m through a given Q. Thus

$$\alpha = (n_1-2)(n_2-2)(m-3)-p(n_1+n_2+m)+9p.$$

The number of united points of this correspondence is the number required.

I show next that $\bar{T}_1$ has valency $3n_1+3n_2-n_1n_2+p-10$. Let R be a given point and consider the γ^1_3 of common trios of $g^2_{n_1}$ and $g^2_{n_2}$. Let S be any one of the remaining points of the groups of γ^1_3 defined by R. Then the correspondence $\bar{T}_2$: (R,S) is of valency n_1+n_2-6 [§ 2]. If $\bar{T}_3$ denote the correspondence (R,P), then $\bar{T}_2+\bar{T}_3$ is of valency

$$(n_1-2)(n_2-2)-p,$$

so that $\bar{T}_3$ has valency $n_1n_2-3n_1-3n_2-p+10$, and, since $\bar{T}_1+\bar{T}_3$ is of valency zero, the result stated follows at once. From the Cayley–Brill formula we now find

$$N[0,1;3] = \tfrac{3}{2}(m-3)(n_1-2)(n_2-2)(n_2-3) -$$
$$-p(n_2-3)(2m+3n_1+n_2-18)+2p(p-1).$$

3.4. LEMMA. *A particular series γ_4^1 and the correspondence generated by it.* The common 4-ads of g_m^3 and $g_{n_2}^2$ form a series γ_4^1 of index ν_4 and with δ_4 double points where

$$\nu_4 = \tfrac{1}{2}(m-3)(n_2-2)(n_2-3)-p(n_2-3).$$

Now $N[0,1;3]$ is the number of common trios of γ_4^1 and $g_{n_1}^2$, so that

$$N[0,1;3] = 3n_1\nu_4-\delta_4,$$

whence

$$\delta_4 = 3(m-3)(n_2-2)(n_2-3)+p(n_2-3)(2m+n_2-18)-2p(p-1).$$

If Q be any one of the points, other than P, of the groups of γ_4^1 defined by a point P, we have a correspondence (P, Q) with indices $(3\nu_4, 3\nu_4)$ and of valency w say.† The united points of this correspondence are the double points of γ_4^1, and, from the Cayley–Brill formula,

$$6\nu_4+2wp = \delta_4,$$

so that
$$w = \tfrac{1}{2}(n_2-3)(2m+n_2-12)-p+1.$$

3.5. *Calculation of* $N[2,3;1]$. Consider the groups of γ_4^1 through a point P. Let the points of these groups, other than P, be points Q and let the complementary groups of γ_4^1 in g_m^3 be points R. Any pair of points R from the same group of g_m^3 defines a group of $g_{n_1}^2$. Let the points of the latter groups, other than the points R, be points S. The points R vary in a series $\bar{\gamma}_{m-4}^1$ of index $\bar{\nu}_4$ and with $\bar{\delta}_4$ double points, where $\bar{\nu}_4$ is the number of common 4-ads of g_{m-1}^2 and $g_{n_2}^2$ so that

$$\bar{\nu}_4 = \tfrac{1}{4}(n_2-2)(n_2-3)(m-3)(m-4)-(n_2-3)(m-4)p+\tfrac{1}{2}p(p-1),$$

while $\bar{\delta}_4$ is the number of groups of g_m^3 having (i) a double point and (ii) a 4-ad in common with $g_{n_2}^2$. To find $\bar{\delta}_4$, consider the groups of $\bar{\gamma}_{m-4}^1$ through a point R and let the remaining points of these groups be points R'. Then the complementary groups of γ_4^1 are the points P corresponding to R; $\bar{\delta}_4$ is the number of united points of (R, R') which has indices $[\bar{\nu}_4(m-5), \bar{\nu}_4(m-5)]$. Now the correspondence (P, R) has valency ν_4-w and it follows that (R, R') has valency $\bar{\nu}_4-\nu_4+w$. Hence

$$\bar{\delta}_4 = 2\bar{\nu}_4(m-5)+2p(\bar{\nu}_4-\nu_4+w).$$

Consider next the correspondence (P, S), which has $N[2,3;1]$ united points, and indices $\left[4\alpha, \nu_4\binom{m-4}{2}(n_1-2)\right]$, where

$$\alpha = (n_1-2)(m-5)\bar{\nu}_4-p(\bar{\nu}_4-\nu_4+w)$$

† As in § 2 (footnote) it is easy to show that this correspondence must possess a valency.

is the number of pairs of points common to $g^1_{n_1-1}$ and $\bar{\gamma}^1_{m-4}$. To find the valency of $\overline{T}_1$, or (P, S), we note that, if $\overline{T}_2$ denotes the correspondence (P, R), then $(m-5)\overline{T}_2+\overline{T}_1$ has valency zero, so that $\overline{T}_1$ has valency $(m-5)(w-\nu_4)$. Hence, by the Cayley–Brill formula,

$$N[2,3;1] = \tfrac{5}{4}(m-3)(m-4)(m-5)(n_1-2)(n_2-2)(n_2-3)-$$
$$-\tfrac{1}{2}(m-4)(m-5)(n_2-3)[9(n_1-2)+4(n_2-3)]p+$$
$$+2(m-5)[n_1-3+3(n_2-3)]p(p-1)-2p(p-1)(p-2).$$

3.6. *Calculation of* $N[1,2;2]$. The groups of $g^2_{n_1}$ through a point P form a $g^1_{n_1-1}$ which has β pairs in common with γ^1_4, where

$$\beta = 3\nu_4(n_1-1)-\tfrac{1}{2}\delta_4.$$

Denote the points of such pairs by Q, the remaining points of the groups of γ^1_4 (other than the points Q), by R, and the remaining points of the groups of g^3_m thus defined, by S. Then $N[1,2;2]$ is the number of united points of the correspondence (P, S), which has indices

$$[6\bar{\nu}_4(n_1-2), \beta(m-4)].$$

Both the correspondences (P, Q) and (P, R) have indices $[3\nu_4(n_1-2), 2\beta]$ and, if we denote the correspondences (P, Q), (P, R), (P, S) by $\overline{T}_1$, $\overline{T}_2$, $\overline{T}_3$ and suppose them to have U_1, U_2, U_3 united points respectively, then $\overline{T}_1+\overline{T}_2+\overline{T}_3$ is of valency zero, and

$$U_1+U_2+U_3 = 6(\nu_4+\bar{\nu}_4)(n_1-2)+m\beta.$$

U_1 is the number of groups of γ^1_4 containing points Q and Q' say, where Q is an ordinary point of $g^2_{n_1}$ while Q' is a double point of the same group of $g^2_{n_1}$. Now Q and Q' correspond (*a*) *via* γ^1_4 in a correspondence with indices $(3\nu_4, 3\nu_4)$ and of valency w, and (*b*) *via* $g^2_{n_1}$, in a correspondence with indices $[n_1-2, 2(n_1+p-2)]$ of valency 2, and U_1 is the number of common corresponding pairs of these last two correspondences, so that

$$U_1 = 3\nu_4(3n_1+2p-6)-4wp.$$

Again, U_2 is three times the number of common trios of γ^1_4 and $g^2_{n_1}$, so that

$$U_2 = 9n_1\nu_4-3\delta_4.$$

We thus find

$$N[1,2;2] = 3(m-3)(m-4)(n_1-2)(n_2-2)(n_2-3)-$$
$$-\tfrac{1}{2}(m-4)(n_2-3)[2m+18n_1+7n_2-72]p+(m+3n_1+6n_2-34)p(p-1).$$

Using the results of §§ 3.4, 3.5 we can find $N[3,4;0]$ by a method

independent of § 3.2, for this number is equally well defined as the number of common trios of $\bar{\gamma}^1_{m-4}$ and $g^2_{n_1}$; thus

$$N[3,4;0] = n_1 \bar{\nu}_4 \binom{m-5}{2} - \tfrac{1}{2}(m-6)\,\bar{\delta}_4.$$

As a final check we have the identity

$$\begin{aligned} &N[3,4;0]+N[2,3;1]+N[1,2;2]+N[0,1;3] \\ &= [\tfrac{1}{2}(m-1)(m-2)(n_1-2)-(m-2)p][\tfrac{1}{4}(m-2)(m-3)(n_2-2)(n_2-3)- \\ &\qquad -(m-3)(n_2-3)p+\tfrac{1}{2}p(p-1)], \end{aligned}$$

the two factors on the right being the respective orders of $V_2(3, n_1)$ and C_2.

REFERENCES

1. G. Castelnuovo, *Rend. Circ. Mat. Palermo*, 3 (1889), 27.
2. A. Comessatti, 'Determinazione dei gruppi di $r+1$ punti comuni ad $r+1$ serie lineari g^r_n', *Atti R. Ist. Veneto*, 69 (1910), 871.
3. V. C. Morton, 'Poristic configurations associated with a rational normal curve', *Proc. Lond. Math. Soc.* (2) 30 (1930), 379.
4. F. Severi, *Trattato di Geometria Algebrica* (Bologna, 1926), 250.
5. R. Torelli, 'Dimostrazione di une formola di de Jonquières e suo significato geometrico', *Rend. Circ. Mat. Palermo*, 21 (1905), 58.
6. ——, 'Sulle serie algebriche di gruppi di punti appartenenti a una curva algebrica', *Atti R. Ist. Veneto*, 67 (1908), 1323.

VALUES OF QUADRATIC FORMS (I)

By A. OPPENHEIM (*Singapore*)

[Received 27 April 1952]

1. I PROVE in this note the following theorems about quadratic forms.

THEOREM 1. *If $f(x_1, x_2, \ldots, x_n)$ is an indefinite quadratic form such that for every $\epsilon > 0$ the inequalities*

$$0 < f(x_1, x_2, \ldots, x_n) < \epsilon$$

are solvable in integers $x_1, x_2, \ldots, x_n$, then if $n \geqslant 3$, the inequalities

$$0 < -f(x_1, x_2, \ldots, x_n) < \epsilon$$

are solvable in integers $x_1, x_2, \ldots, x_n$ for every positive ϵ.

This theorem need not be true for $n = 2$. It is quite easy to show this by using the chain of reduced forms determined by a given indefinite binary quadratic form $f(x, y)$. But, as a direct proof is available by simple continued fractions, I give it for the sake of completeness.

LEMMA 1. *Suppose that the irrational number $\omega > 1$ is given by the simple continued fraction*

$$\omega = [a_1, a_2, \ldots, a_n, \ldots] \quad (a_n \geqslant 1, \text{ integral}) \tag{1.1}$$

with convergents p_n/q_n, then

$$p_i q_i - \omega q_i^2 = (-1)^i \delta_i \quad (i = 1, 2, \ldots), \tag{1.2}$$

where

$$\frac{1}{2+a_{i+1}} < \delta_i < \frac{1}{a_{i+1}}. \tag{1.3}$$

For, if $\omega_{i+1} = [a_{i+1}, a_{i+2}, \ldots]$, then

$$\frac{p_i}{q_i} - \omega = \frac{p_i}{q_i} - \frac{p_i \omega_{i+1} + p_{i-1}}{q_i \omega_{i+1} + q_{i-1}} = \frac{(-1)^i}{q_i^2} \delta_i,$$

where

$$\frac{1}{\delta_i} = \omega_{i+1} + \frac{q_{i-1}}{q_i},$$

so that

$$1/\delta_i < a_{i+1} + 1 + 1, \qquad 1/\delta_i > a_{i+1}.$$

LEMMA 2. *If, for integers p and q,*

$$0 < |pq - \omega q^2| \leqslant \tfrac{1}{2}, \tag{1.4}$$

then p/q is a convergent to ω.

This is a classical theorem of Legendre's.

Now take the integers a_i to satisfy the following conditions

$$1 \leqslant a_{2i} \leqslant h \text{ (all } i), \qquad \limsup a_{2i+1} = \infty. \tag{1.5}$$

Quart. J. Math. Oxford (2), 4 (1953), 54–59.

Plainly the inequalities

$$0 < pq-\omega q^2 < \epsilon \tag{1.6}$$

are solvable in integers p, q for every positive ϵ. For we may take $p = p_{2i}$, $q = q_{2i}$, where i runs through the sub-sequence (i) such that $a_{2i+1} \to \infty$, so that

$$0 < p_{2i}q_{2i}-\omega q_{2i}^2 = \delta_{2i} \to 0.$$

On the other hand the inequalities

$$0 < -(pq-\omega q^2) < \epsilon \tag{1.7}$$

are not solvable in integers p, q if

$$0 < \epsilon < 1/(h+2). \tag{1.8}$$

For Lemma 2 shows that, if these inequalities hold, p/q must be a convergent to ω and, moreover, by Lemma 1 an *odd* convergent. Thus we have

$$\begin{aligned} -(pq-\omega q^2) &= -(-1)^j\delta_j g^2 \quad (j \text{ odd}) \\ &\geqslant \delta_j > 1/(h+2), \end{aligned}$$

where g is the greatest common divisor of p and q.

Thus *the indefinite binary quadratic form*

$$f(x,y) = xy-\omega y^2,$$

where the irrational number $\omega > 1$ satisfies the conditions that its even-placed partial quotients are bounded and its odd-placed partial quotients are unbounded, is such that

$$0 < f(x,y) < \epsilon$$

is solvable in integers for every $\epsilon > 0$ but

$$0 < -f(x,y) < \epsilon$$

is NOT *solvable in integers x and y for every positive ϵ.*

This form $f(x,y)$ represents zero. But it is clear that it is equally simple to construct non-zero forms with the same properties.

Theorem 1 is an immediate deduction from

THEOREM 2. *If f is an indefinite form with non-zero determinant $\Delta(f)$, then to every positive value a taken by $f(x)$ there corresponds a negative value $-b$ taken by $f(x)$ such that*

$$b^{2n-2} \leqslant A_n a^{n-2}|\Delta(f)|,$$

where the constant A_n depends only on n.

Both a and b can be properly represented values.

It is convenient to prove Theorem 2 together with

THEOREM 3. *If $P_1(f)$ denotes the lower bound of the positive values of a positive definite or indefinite form f, then*

$$P_1^n(f) \leqslant B_n|\Delta(f)|,$$

where B_n is a constant which depends only on n.

Theorems 1 and 2 are new. Theorem 3 is of course classical for definite forms. For indefinite forms we owe the ternary case to Davenport (**2**) who obtained the best value of B_3 for $\Delta > 0$ and for $\Delta < 0$ and the general case to Blaney (**1**).

Here I prove Theorems 2 and 3 together by induction, assuming each to hold for $n-1$. Later I give another proof of Theorem 2, depending on ideas due to Korkine and Zolotareff, which gives the inequality

$$B_n \leqslant B_{n-1}^{n/(n-2)}.$$

2. For $n = 2$, Theorem 2 reduces to Theorem 3 applied to the indefinite form $-f$; and Theorem 3 for a positive definite binary form is classical with $B_2 = \frac{4}{3}$, while for an indefinite form f it is simply a deduction from the existence of a reduced form

$$\alpha x^2+\beta xy-\gamma y^2$$

with $$\alpha > 0, \qquad \gamma > 0, \qquad \alpha+\gamma \leqslant d,$$

where d^2 $(d > 0)$ is the discriminant unless $f \sim dxy$, in which case $P_1(f) = d$.

3. Assume now that Theorem 3 holds for $n-1$ variables, where $n \geqslant 3$. If the integers such that $f(x) = a > 0$ have greatest common divisor $g > 1$, it will be sufficient to prove the theorem for a/g^2 which is properly represented. Hence, supposing that a is properly represented, we obtain by a unimodular transformation

$$f \sim a(x_1+\ldots)^2+\phi(x_2,\ldots,x_n) \tag{3.1}$$

on completing the square, where

$$a\,\Delta(\phi) = \Delta(f).$$

Suppose first that f is indefinite. Then the form $-\phi$ is positive-definite or indefinite. Hence, by Theorem 3 for $n-1$, integers $x_2,\ldots, x_n$ exist with

$$0 < -\phi = c, \qquad 0 < c^{n-1} \leqslant B_{n-1}|\Delta(\phi)|(1+\epsilon) \tag{3.2}$$

for assigned positive ϵ. But now the form $f(x_1, x_2t, x_3t,\ldots, x_nt)$ is an indefinite binary form in x_1 and t with determinant $-ac$ and therefore represents properly a number $-b < 0$ such that

$$0 < b \leqslant 2(ac)^{\frac{1}{2}}. \tag{3.3}$$

Hence $$b^{2n-2} \leqslant 2^{2n-2}B_{n-1}a^{n-2}|\Delta(f)|(1+\epsilon), \tag{3.4}$$

which proves Theorem 2 for n with $A_n = 2^{2n-2}B_{n-1}$.

Theorem 3 for indefinite forms f_n now follows from Theorem 2 since we may choose a so that

$$P_1(f) \leqslant a \leqslant P_1(f)+\epsilon$$

for any positive ϵ. It follows that

$$P_1^{2n-2}(-f) \leqslant A_n P_1^{n-2}(f)|\Delta(f)|. \tag{3.5}$$

Apply this to the indefinite form $-f$ with determinant

$$\Delta(-f) = (-1)^n\Delta(f).$$

Then

$$P_1^{2n-2}(f) \leqslant A_n P_1^{n-2}(-f)|\Delta(f)|. \tag{3.6}$$

From (3.5) and (3.6) we deduce that

$$P_1^{(2n-2)^2} \leqslant (A_n|\Delta|)^{2n-2}(A_n P_1^{n-2}|\Delta|)^{n-2}, \qquad P_1^{3n^2-4n} \leqslant A_1^{3n-4}|\Delta|^{3n-4},$$

$$P_1^n(f) \leqslant B_n|\Delta(f)|,$$

with

$$B_n = A_n = 2^{2n-2}B_{n-1}$$

when f is indefinite.

To complete the induction we ought to show that Theorem 3 holds also for positive definite forms in n variables when it holds in $n-1$ variables. Naturally, the argument now is classical. The form ϕ in (3.1) is positive-definite:

$$\phi(x_1,\ldots,x_n) = c > 0, \qquad c^{n-1} \leqslant B_{n-1}|\Delta(\phi)|(1+\epsilon).$$

The binary form $f(x_1, x_2 t,\ldots, x_n t)$ in x_1 and t is positive definite and represents $a_1 > 0$ such that

$$a_1^2 \leqslant \tfrac{4}{3}ac,$$

and, as before,

$$a_1^{2n-2} \leqslant A_n a^{n-2}|\Delta(f)|,$$

whence we have Theorem 3 for positive definite forms in n variables.

4. An entirely different proof of Theorem 3 will now be given. It leads to the inequality

$$B_n \leqslant B_{n-1}^{n/(n-2)}, \tag{4.1}$$

an inequality proved for definite forms by Korkine and Zolotareff (**1**) when $n = 4$. Their argument was employed for indefinite quaternary forms of signature zero in 1929 (Oppenheim **4**) and for the general definite form by Mordell (**3**) in 1944 [see also Oppenheim (**5**)]. Modifications are needed since the sections of an indefinite form may be definite or indefinite. We observe, however, that a form $f(x_1, x_2,\ldots, x_n)$ cannot be negative-definite if its determinant has the sign of $(-1)^{n-1}$.

The form

$$f = \sum a_{ik}x_i x_k \quad (a_{ik} = a_{ki}) \tag{4.2}$$

has the adjoint

$$F = \sum A_{ik}X_i X_k, \tag{4.21}$$

where A_{ik} is the cofactor of a_{ik} in $\Delta(f)$. If

$$f \sim g = \sum b_{ik} y_i y_k \tag{4.22}$$

by the transformation

$$x_i = \sum c_{ij} y_j, \qquad |c_{ij}| \neq 0, \tag{4.23}$$

then

$$F \sim G = \sum B_{ik} Y_i Y_k, \tag{4.24}$$

where G is the adjoint of g, by the contragredient transformation

$$X_i = \sum C_{ij} Y_j, \tag{4.25}$$

where C_{ij} is the cofactor of c_{ij} in (c_{ij}) of determinant 1. The converse is also true.

Suppose now that F represents properly the number A for integers $c_1,..., c_n$ with greatest common divisor unity. These integers can be taken as the *first column* in a unimodular matrix (C_{ij}). Thus $F \sim G$ in which $B_{11} = A$ and B_{11} is the *determinant* of the $(n-1)$ary section

$$g(0, y_2,..., y_n) \tag{4.26}$$

of $g(y)$ formed by putting $y_1 = 0$. It follows that any number A properly represented by the adjoint F is the determinant of some $(n-1)$ary section of f.

To determine whether this section is positive-definite or indefinite it is enough to put f and F into *diagonal* form,

$$f \sim d_1 y^2 + d_2 y_2^2 + ... + d_n y_n^2, \qquad F \sim D_1 Y_1^2 + ... + D_n Y_n^2 \tag{4.27}$$

with $A = D_1 = d_2 d_3 ... d_n$.

If f is positive-definite, then F is positive-definite. The $(n-1)$ary section

$$h = d_2 y_2^2 + ... + d_n y_n^2 \tag{4.28}$$

of determinant A is positive-definite.

If f is indefinite, then F is indefinite. Suppose that $(-1)^n A > 0$. Then the determinant of the $(n-1)$ary form h in (4.28) has the sign of $(-1)^{n-2}$. Hence h is positive-definite or indefinite, for, if it were negative definite, its determinant must have the sign of $(-1)^{n-1}$.

Thus any number A properly represented by F and such that $(-1)^n A > 0$ when f is indefinite is the determinant of an $(n-1)$ary section of f which is positive definite or indefinite. Write

$$\delta = \begin{cases} 1 & (f \text{ positive-definite}), \\ (-1)^n & (f \text{ indefinite}), \end{cases} \tag{4.3}$$

so that δA *is a positive value* of δF.

Apply Theorem 3 for $(n-1)$ary forms to the section of which A is the determinant, noting that every positive value of the section is a positive value of f. Hence

$$P_1^{n-1}(f) \leqslant B_{n-1}|A|,$$

and hence

$$P_1^{n-1}(f) \leqslant B_{n-1} P_1(\delta F). \tag{4.4}$$

The inequality (4.4) applies to the form δF (which is positive definite or indefinite) with adjoint

$$\delta^{n-1}\Delta^{n-2}(f).f = \Delta^{n-2}f, \tag{4.5}$$

so that

$$P_1^{n-1}(\delta F) \leqslant B_{n-1} P_1\{\delta\Delta^{n-2}f\},$$

i.e.

$$P_1^{n-1}(\delta F) \leqslant B_{n-1}|\Delta|^{n-2} P_1(\delta\delta' f), \tag{4.6}$$

where

$$\delta' = 1 \quad (\Delta > 0), \qquad \delta' = (-1)^{n-2} \quad (\Delta < 0). \tag{4.7}$$

From (4.4) and (4.6) we get

$$P_1^{(n-1)^2}(f) \leqslant B_{n-1}^n|\Delta|^{n-2} P_1(\delta\delta' f), \tag{4.8}$$

which gives the required result if $\delta\delta' = 1$. If, however, $\delta\delta' = -1$ (which can happen only for indefinite f), we get

$$P_1^{(n-1)^2}(f) \leqslant B_{n-1}^n|\Delta|^{n-2} P_1(-f),$$

which applied to the indefinite form $-f$ gives

$$P_1^{(n-1)^2}(-f) \leqslant B_{n-1}^n|\Delta|^{n-2} P_1(f).$$

Plainly the same result is reached as before by eliminating $P_1(-f)$.

5. A stronger inequality than that contained in Theorems 2 and 3 can be given if we exclude forms f equivalent to

$$M\{x_1 x_2 + \phi(x_3, \ldots, x_n)\},$$

where ϕ has *integral* coefficients. Excluding such forms, *we have for any indefinite form*

$$(P_1 + P_2)^{2n-2} \leqslant C_1(n, s) P_1^{n-2}|\Delta(f)|,$$

where $C_1(n, s)$ denotes a constant which depends on n and on s, the signature of the form, and $P_2(f) = P_1(-f)$.

REFERENCES

1. H. Blaney, 'Indefinite quadratic forms in n variables', *J. London Math. Soc.* 23 (1948), 153–60.
2. H. Davenport, 'On indefinite ternary quadratic forms', *Proc. London Math. Soc.* (2) 51 (1949), 145–60.
3. L. J. Mordell, 'A positive quadratic form in eight variables', *J. London Math. Soc.* 19 (1944), 3–6.
4. A. Oppenheim, 'The minimum of indefinite quaternary quadratic forms of signature zero', *Proc. National Acad. of Sciences*, 15 (1929), 724–7.
5. —— 'Remark on the minimum of quadratic forms', *J. London Math. Soc.* 21 (1946), 251–2.

VALUES OF QUADRATIC FORMS (II)

By A. OPPENHEIM (*Singapore*)

[Received 27 April 1952]

1. It is known after Meyer [for a proof and references see Dickson (**3**)] that an integral indefinite quadratic form in five or more variables must represent zero properly, i.e. for integral values of the variables which are not all zero. It has been conjectured that, if f is an incommensurable form in five or more variables, then the inequality

$$0 < |f(x_1, x_2, \ldots, x_n)| < \epsilon \tag{1.1}$$

is solvable for every positive ϵ in integers $x_1, \ldots, x_n$ not all zero, the determinant of the form $\Delta(f)$ not being zero.

If f takes special forms, something can be proved. Thus for any positive irrational θ the inequalities

$$0 < \theta x^2 - y^2 - z^2 - t^2 < \epsilon$$

are solvable in integers x, y, z, t for every positive ϵ.

With suitable restrictions on the coefficients c_j, Chowla (**1**) established the solvability of the inequalities

$$0 < \Big| \sum_1^9 c_j x_j^2 \Big| < \epsilon,$$

and recently Davenport and Heilbronn (**2**) have replaced 9 by 5 and moreover require merely one irrationality in the ratios $c_1 : c_2 : \ldots : c_5$. (But it may be remarked in passing that, if only one irrationality occurs, the number 5 may be replaced by 4). In an unpublished note, G. L. Watson has extended the work of Davenport and Heilbronn to include one cross-product.

In this note I prove the following

THEOREM 1. *If the indefinite form f in n ($\geqslant 5$) variables and non-zero determinant represents zero properly and is not a multiple of a rational form, then the inequalities*

$$0 < |f(x_1, x_2, \ldots, x_n)| < \epsilon$$

are solvable in integers $x_1, \ldots, x_n$ for every positive ϵ.

Otherwise expressed, let $M(f)$ be the lower bound of the non-zero values of $|f|$ so that $f \neq 0$ implies $|f| \geqslant M$. Then, *if* (i) *f is a zero form*, (ii) $M > 0$, (iii) $n \geqslant 5$, *the form f must be a multiple of a rational form.*

This result I feel sure is true even for $n = 3$, although it is obviously false for $n = 2$. It then reduces, as the analysis will show, to this question: *given an irrational θ, are the inequalities*

$$0 < |xy+\theta y^2-z^2| < \epsilon$$

solvable in integers x, y, z for every positive ϵ?

The proof of Theorem 1 employs (1) Diophantine approximations for the fractional parts of $m\theta$, $m^2\theta$ where m is integral, (2) properties of a genus of ternary quadratic forms with integral coefficients.

2. We consider the hypotheses (i) that the form

$$f = \sum a_{ik}x_i x_k \quad (a_{ki} = a_{ik};\ \Delta \neq 0) \tag{2.1}$$

represents zero properly and (ii) $M(f) > 0$, i.e. there exists a number $M > 0$ such that $|f| \geqslant M$ whenever $f \neq 0$.

THEOREM 2. *If there exists in n variables a form f satisfying hypotheses* (i) *and* (ii), *then there exists a form*

$$F = h(X_1X_2+\theta X_2^2+c_3X_3^2+c_4X_4^2+\ldots+c_nX_n^2)$$

such that $M(F) > 0$ in which $c_3,\ldots, c_n$ are integers different from zero. The number θ may or may not be irrational. The form F will be derived from f by rational non-singular transformations.

The proof is conveniently given in a series of lemmas.

LEMMA 1. *After an appropriate unimodular transformation we may suppose that*

$$a_{11} = 0,\ a_{13} = a_{14} = \ldots = a_{1n} = 0, \quad a_{12} \neq 0.$$

Since f represents zero properly, we have

$$f \sim g = \sum b_{ik}y_iy_k \quad (b_{11} = 0).$$

If $b_{12}:b_{13}:\ldots:b_{1n}$ are not all rational, integers $y_2,\ldots, y_n$ exist such that

$$0 < |b_{12}y_2+\ldots+b_{1n}y_n| < \epsilon,$$

and now integral y_1 can be found so that

$$0 < |g(y_1, y_2,\ldots, y_n)| \leqslant 2\epsilon,$$

a contradiction if $2\epsilon < M(g) = M(f)$.

Thus we may write

$$b_{1i} = hp_{1i} \quad (i = 2,\ldots, n),$$

where (i) $h \neq 0$, (ii) $p_{12},\ldots, p_{1n}$ are integers with greatest common divisor unity (since $\Delta(f) \neq 0$). There exists therefore a unimodular transformation on $y_2,\ldots, y_n$ which keeping y_1 fixed replaces $p_{12}y_2+\ldots+p_{1n}y_n$ by z_2. This proves the lemma. We now have

$$f = 2a_{12}x_1x_2+a_{22}x_2^2+2a_{23}x_2x_3+\ldots+2a_{2n}x_2x_n+\phi(x_3,\ldots,x_n), \quad (2.2)$$

where $\Delta(f) = -a_{12}^2\Delta(\phi), \qquad a_{12} \neq 0, \qquad \Delta(\phi) \neq 0.$

LEMMA 2. *If one of θ_1, θ_2 is irrational, then, for assigned positive ϵ, the inequality*

$$|n^2\theta_1+n\theta_2-m-\alpha| < \epsilon$$

has an infinity of solutions in integers n and m.

This result is deducible from theorems given by Hardy and Littlewood (**4**). It is a special case of a general theorem given by Weyl (**9**).

LEMMA 3. *If $M(f) > 0$, the coefficients of the form $\phi(x_3,\ldots,x_n)$ in (2.2) are rational multiples of a_{12}.*

Suppose for example that a_{33}/a_{12} is irrational. Consider (with $2a_{12} = 1$ to save writing)

$$f(x_1, 1, x_3, 0,\ldots) = x_1+a_{22}+2a_{23}x_3+a_{33}x_3^2.$$

By Lemma 2 for an infinity of integers x_3, x_1

$$|x_1+a_{22}+2a_{23}x_3+a_{33}x_3^2| < \epsilon.$$

The left-hand side cannot vanish more than three times since a_{33} is irrational. Hence $M(f) < \epsilon$ for every positive ϵ, a contradiction.

Thus (with $2a_{12} = 1$) a_{33} is irrational, i.e. *every value* assumed by ϕ is a rational multiple of a_{12}. Lemma 3 is proved.

LEMMA 4. *If $M(f) > 0$, the coefficients $a_{23},\ldots, a_{2n}$ are rational multiples of a_{12}.*

As before take $2a_{12} = 1$ and consider

$$f(x_1, 1, x_3, 0,\ldots) = x_1+a_{22}+2a_{23}x_3+a_{33}x_3^2.$$

Lemma 2 yields a contradiction if a_{23} is irrational.

LEMMA 5. *If $M(f) > 0$, the only possible irrational ratio in the coefficients of f is a_{22}/a_{12}.*

This is obvious from Lemmas 3 and 4.

LEMMA 6. *Suppose that the form g has $M(g) > 0$. Then any form h derived from g by a non-singular rational (not necessarily integral) transformation has $M(h) > 0$.*

If, however, $M(g) = 0$, then $M(h) = 0$ and conversely.

By hypothesis a transformation

$$\sigma x_i = \sum_{j=1}^{n} p_{ij}y_j \quad (i = 1,\ldots, n)$$

with integral σ, p_{ij} carries $g(x)$ into $h(y)$. Consider any set of integers y_j (not all zero). Then plainly

$$\sigma^2h(y_j) = h(\sigma y_j) = g(p_{ij}y_j),$$

a value of $g(x)$ *for integral* x. It follows that

$$\sigma^2 M(h) \geqslant M(g),$$

from which the Lemma follows.

Proof of Theorem 2. The hypotheses (i) f represents zero and (ii) $M(f) > 0$ have given us a form f in (2.2) in which by Lemmas 3, 4 the ratios a_{2j}/a_{12} $(j = 3,..., n)$ are all rational and the coefficients of $\phi(x_3,..., x_n)/a_{12}$ are all rational.

Now by rational transformations we can reduce ϕ to the form

$$2a_{12}(c_3 y_3^2 + ... + c_n y_n^2)$$

with integral coefficients $c_3,..., c_n$. This will give us a form

$$g = 2a_{12}[x_1 x_2 + bx_2^2 + 2b_{23} x_2 y_3 + ... + 2b_{2n} x_2 y_n + c_3 y_3^2 + ... + c_n y_n^2]$$

with $M(g) > 0$ (Lemma 6) and $b_{23},..., b_{2n}$ all rational. Now replace x_1 by $y_1 - 2b_{23} y_3 - ... - 2b_{2n} y_n$ and x_2 by y_2 to obtain Theorem 2 (by another application of Lemma 6). The form F is derived from f by rational non-singular transformations.

3. THEOREM 3. *If* θ *is irrational and* $c_3,..., c_n$ *are integral, then, if* $n \geqslant 5$, *the inequalities*

$$0 < |X_1 X_2 + \theta X_2^2 + c_3 X_3^2 + ... + c_n X_n^2| < \epsilon$$

are solvable for every ϵ *in integers* $X_1,..., X_n$.

To illustrate the proof I take a simple case,

$$f = \theta x^2 - y^2 - z^2 - t^2$$

with positive irrational θ. By Lemma 2 we can solve

$$|\tfrac{1}{8}\theta x^2 - n - \tfrac{1}{8}| < \epsilon$$

for any positive ϵ in integers x and n. Now the form $y^2 + z^2 + t^2$ represents all members of the arithmetic progression $8n + 1$. Thus for each positive ϵ, integers x, y, z, t exist with

$$0 < |\theta x^2 - y^2 - z^2 - t^2| < 8\epsilon.$$

In proving Theorem 3 we may suppose that $n = 5$. We need to extend to any integral ternary quadratic form the result just used for $y^2 + z^2 + t^2$.

LEMMA 7. *If* $Q(x, y, z)$ *is an integral ternary quadratic form (definite or indefinite) with non-zero determinant, then there exists an arithmetic progression* $Ah + B$ *such that*

$$Q(x, y, z) = Ah + B \quad (A \neq 0)$$

is solvable in integers x, y, z *for every integer* h. (*Naturally* $Ah + B > 0$ *if* Q *is positive definite*).

This important Lemma is deducible from theorems due to Smith (**8**), Jones (**5**), (**6**), and Ross (**7**).

The argument employed in the proof of Lemma 6 shows that it is enough to prove Lemma 7 for any form derived from Q by a rational non-singular transformation. Thus we suppose that

$$Q = a(px^2+qy^2+rz^2)$$

where the integers p, q, r are squarefree and coprime in pairs and a is an integer. It is sufficient to consider $a = 1$.

The form Q under unimodular transformations belongs to a class C of equivalent forms. This class C belongs to a genus G which contains a finite number of classes $C = C_1, C_2,..., C_n$ $(n \geqslant 1)$. *Any form Q_i in the class C_i is transformable into any form Q_j in the class C_j by a rational non-singular transformation of determinant unity, the denominator of which is prime to $2D$ (D being the determinant of the forms).* [Smith (**8**).]

This fundamental property may be taken as the definition of a genus.

Next *there exists an arithmetic progression $Ah+B$ such that, for every integer h there is a form Q_i which represents $Ah+B$.* [Jones (**5**), (**6**) 116, for definite forms: as Jones remarks, his methods apply also to indefinite forms; Ross (**7**) for indefinite forms.]

Naturally $Ah+B > 0$ if Q is positive-definite.

Let $Q_1 = Q, Q_2,..., Q_n$ be forms which represent the classes $C_1, C_2,..., C_n$ in the genus G. The number $Ah+B$ is represented by Q_i so that

$$Q_i(X, Y, Z) = Ah+B$$

for appropriate integers X, Y, Z. There exists a rational transformation of determinant unity which carries $Q_i(\xi, \eta, \zeta)$ into $Q_1(x, y, z) = Q$. If we suppose that the integers ξ, η, ζ are integral multiples of an appropriate fixed integer σ_i, then x, y, z will also be integers: we obtain

$$Q(x, y, z) = Q_i(\sigma_i X, \sigma_i Y, \sigma_i Z) = \sigma_i^2(Ah+B)$$

for integers x, y, z.

Let σ be the least common multiple of the integers σ_i $(i = 2,..., n)$. Plainly Q represents the integer $\sigma^2(Ah+B)$; thus Q represents all members of the arithmetic progression $(A\sigma^2)h+(B\sigma^2)$ (these numbers being positive if Q is positive-definite).

Proof of Theorem 3. Apply Lemma 7 to the integral form

$$\phi = c_3 X_3^2+c_4 X_4^2+c_5 X_5^2,$$

where c_3, c_4, c_5 are integers different from zero. Integers A (of the same

sign as $c_3c_4c_5$) and B exist such that ϕ represents $Ah+B$ for all large positive integers h. By Lemma 2 the inequality

$$\left|\frac{\theta}{A}X_2^2-m+\frac{B}{A}\right|<\epsilon$$

has an infinity of solutions in integers X_2, m for every positive ϵ. We may write therefore

$$\theta X_2^2-mA+B=\delta$$

with $|\delta|<|A|\epsilon$ for infinitely many integers X_2 and m. Take $X_1=-Ax_1$ (x_1 integral): then

$$X_1X_2+\theta X_2^2+c_3X_3^2+c_4X_4^2+c_5X_5^2$$
$$=-\{(x_1X_2-m)A+B\}+\phi(X_3,X_4,X_5)+\delta.$$

The integer x_1 can be chosen so that $h=x_1X_2-m>0$: now choose integers X_3, X_4, X_5 so that $\phi=Ah+B$, which is possible if h is sufficiently large. Thus for infinitely many sets of integers ($X_2\neq 0$) the inequality

$$|X_1X_2+\theta X_2^2+c_3X_3^2+c_4X_4^2+c_5X_5^2|<\epsilon$$

is solvable if θ is irrational. Vanishing is excluded by the irrationality of θ. This proves Theorem 3.

4. Theorem 3 shows that, for a form f in five or more variables which satisfies the conditions of Theorem 2, the number θ must be rational: i.e., if (i) f represents zero properly, (ii) there exists a positive constant M such that $f\neq 0$ implies $|f|\geqslant M$, then f must be a multiple of a form with rational coefficients.

For $n=4$ we have this question. *Is it or is it not true that, if θ is irrational and a and b are integers, the inequalities*

$$0<|xy+\theta y^2-az^2-bt^2|<\epsilon$$

are solvable in integers x, y, z, t for every positive ϵ?

For $n=3$ the question reduces to this: *if θ is irrational, are the inequalities*

$$0<|xy+\theta y^2-z^2|<\epsilon$$

solvable in integers x, y, z for every positive ϵ?

It may be pointed out that in another (unpublished) paper with the same title I have shown that the solvability of

$$0<f(x_1,\ldots,x_n)<\epsilon$$

for every positive ϵ involves the solvability of

$$-\epsilon<f(x_1,\ldots,x_n)<0$$

for every positive ϵ provided that $n\geqslant 3$.

REFERENCES

1. S. Chowla, 'A theorem on irrational indefinite quadratic forms', *J. London Math. Soc.* 9 (1934), 162–3.
2. H. Davenport and H. Heilbronn, 'On indefinite quadratic forms in five variables', ibid. 21 (1946), 185–93.
3. L. E. Dickson, *Studies in the Theory of Numbers* (Chicago, 1930).
4. G. H. Hardy and J. E. Littlewood, 'Some problems of Diophantine approximation', *Acta Math.* 37 (1914), 155–90.
5. B. W. Jones, 'A new definition of genus for ternary quadratic forms', *Trans. American Math. Soc.* 33 (1931), 92–110.
6. —— 'The regularity of a genus of positive ternary quadratic forms', ibid. 33 (1931), 111–24.
7. A. E. Ross, 'On representation of integers by quadratic forms', *Proc. Nat. Ac. Sc.* 18 (1932), 600–8.
8. H. J. S. Smith, 'On the orders and genera of ternary quadratic forms', *Collected Math. Papers* (Oxford, 1894), (I) 455–506.
9. H. Weyl, 'Über die Gleichverteilung von Zahlen mod Eins', *Math. Ann.* 77 (1916), 313–52.

HILBERT'S FUNCTION IN A LOCAL RING

By D. G. NORTHCOTT (*Cambridge*)

[Received 3 June 1952]

1. Introduction

SUPPOSE that K is a field and that $\mathfrak{a}$ is a homogeneous ideal in the polynomial ring $K[X_0, X_1, \ldots, X_n] = K[X]$. If $\mathfrak{f}(r, \mathfrak{a})$ is the vector space over K consisting of all the forms of degree r contained in $\mathfrak{a}$ and if $\mathfrak{f}(r)$ is the vector space of all forms of degree r, then

$$\chi(r, \mathfrak{a}) = \dim_K \mathfrak{f}(r) - \dim_K \mathfrak{f}(r, \mathfrak{a}) \tag{1.1}$$

is called the *Hilbert function* of $\mathfrak{a}$. It has a number of important properties some of which will be recalled later. Let us now pass to the ring of quotients of $K[X]$ with respect to the prime ideal $(X_0, X_1, \ldots, X_n)$. This ring of quotients, which I shall denote by Q, is a local ring with $\mathfrak{m} = Q(X_0, X_1, \ldots, X_n)$ as its maximal ideal; also, since $\mathfrak{a}$ is homogeneous, if we write $\mathfrak{a}' = Q\mathfrak{a}$, then $\mathfrak{a}' \cap K[X] = \mathfrak{a}$. Let $\theta \in \mathfrak{a}' \cap \mathfrak{m}^r$ then

$$\theta = \frac{\psi_r(X) + \psi_{r+1}(X) + \ldots + \psi_s(X)}{\omega(X)} \tag{A}$$

where $\psi_i(X)$ is a *form* of degree i in $X_0, X_1, \ldots, X_n$ and where $\omega(X)$ is a polynomial such that $\omega(0) = \omega(0, 0, \ldots, 0) \neq 0$. Further,

$$\psi_r(X) + \psi_{r+1}(X) + \ldots + \psi_s(X) = \omega(X)\theta \in \mathfrak{a}' \cap K[X] = \mathfrak{a}$$

and therefore, since $\mathfrak{a}$ is homogeneous, $\psi_r(X) \in \mathfrak{a}$ and $\psi_r(X)/\omega(0) \in \mathfrak{f}(r, \mathfrak{a})$. It is easily verified that the form $\psi_r(X)/\omega(0)$ is determined solely by θ and is independent of the representation (A), and it is also easily verified that the mapping $\theta \to \psi_r(X)/\omega(0)$ is a linear mapping, with respect to K, of $\mathfrak{a}' \cap \mathfrak{m}^r$ on to $\mathfrak{f}(r, \mathfrak{a})$. In addition, θ is mapped into zero if and only if $\psi_r(X)$ is the null form: that is to say if and only if $\theta \in \mathfrak{a}' \cap \mathfrak{m}^{r+1}$. This shows that

$$\dim_K \mathfrak{f}(r, \mathfrak{a}) = \dim_K(\mathfrak{a}' \cap \mathfrak{m}^r / \mathfrak{a}' \cap \mathfrak{m}^{r+1})$$

and (as a special case)

$$\dim_K \mathfrak{f}(r) = \dim_K \mathfrak{m}^r / \mathfrak{m}^{r+1}.$$

Accordingly, if we write $\chi(r, \mathfrak{a}') = \chi(r, \mathfrak{a})$, then

$$\chi(r, \mathfrak{a}') = \dim_K\{\mathfrak{m}^r/\mathfrak{m}^{r+1}\} - \dim_K\{\mathfrak{a}' \cap \mathfrak{m}^r/\mathfrak{a}' \cap \mathfrak{m}^{r+1}\}. \tag{1.2}$$

This formula together with

$$K = Q/\mathfrak{m} \tag{1.3}$$

provides a means of extending the definition of the *characteristic* or

Hilbert function $\chi(r, \mathfrak{a})$ so as to make it applicable to an arbitrary ideal in a general local ring. It is the purpose of the present paper to lay the foundations of a theory of the generalized Hilbert function. The idea that such a generalization can be found was suggested by the algebraic theory contained in the first two chapters of P. Samuel's thesis (**2**), and in § 3 of this discussion† will be found the precise connexion between the Hilbert function as defined here and Samuel's function $P_{\mathfrak{q}}(n)$. In order to relate the results which will shortly be obtained to those of Samuel's, however, it is convenient not to use the formulae (1.2) and (1.3) as they stand, but to carry the generalization yet one stage further in a manner which must now be explained.

2. The generalized Hilbert function

Let Q be a local ring, $\mathfrak{m}$ its maximal ideal, and let $\mathfrak{q}$ be an $\mathfrak{m}$-primary ideal; then $A = Q/\mathfrak{q}$ is a primary ring: that is to say A is a Noetherian ring which has only one proper prime ideal, namely $\mathfrak{p} = \mathfrak{m}/\mathfrak{q}$. As is well known, A has a definite length l. This means that we can find a decreasing chain

$$\mathfrak{p} = \mathfrak{c}_1 \supset \mathfrak{c}_2 \supset \ldots \supset \mathfrak{c}_l = (0)$$

of l ideals, stretching from $\mathfrak{p}$ to (0), such that for each i there is no ideal strictly between $\mathfrak{c}_i$ and $\mathfrak{c}_{i+1}$. Suppose now that $\mathfrak{M}$ is some finitely generated A-module, say

$$\mathfrak{M} = A\mu_1 + A\mu_2 + \ldots + A\mu_h.$$

If $\mu_1, \mu_2, \ldots, \mu_h$ are independent, i.e. if $\alpha_1\mu_1 + \alpha_2\mu_2 + \ldots + \alpha_h\mu_h = 0$, where $\alpha_i \in A$, only when all the α_i are zero, then a composition series composed of submodules of $\mathfrak{M}$ will contain exactly hl terms;‡ if $\mu_1, \mu_2, \ldots, \mu_h$ are not independent, a composition series of submodules of $\mathfrak{M}$ will contain fewer than hl terms. Let us denote the number of terms in a composition series for $\mathfrak{M}$ by $\dim_A \mathfrak{M}$; then, for example, if $\mathfrak{q} = \mathfrak{m}$, A will be a field and $\dim_A \mathfrak{M}$ will have its usual meaning. Note that, if $\mathfrak{N}_1$ and $\mathfrak{N}_2$ are submodules of $\mathfrak{M}$, with respect to A, then

$$\dim_A(\mathfrak{N}_1 + \mathfrak{N}_2) + \dim_A(\mathfrak{N}_1 \cap \mathfrak{N}_2) = \dim_A \mathfrak{N}_1 + \dim_A \mathfrak{N}_2 \qquad (2.1)$$

because, using a familiar theorem on isomorphisms,

$$\begin{aligned} \dim_A(\mathfrak{N}_1 + \mathfrak{N}_2) - \dim_A \mathfrak{N}_1 &= \dim_A(\mathfrak{N}_1 + \mathfrak{N}_2)/\mathfrak{N}_1 \\ &= \dim_A \mathfrak{N}_2/(\mathfrak{N}_1 \cap \mathfrak{N}_2). \end{aligned}$$

To define the Hilbert function we proceed as follows. Let $\mathfrak{a}$ be an

† See, in particular, Theorem 1, Corollary 2.

‡ In counting the number of terms in a composition series for $\mathfrak{M}$ we exclude $\mathfrak{M}$ itself but include the module (0).

arbitrary ideal of Q. Then for any $r \geqslant 0$ we have $\mathfrak{q}(\mathfrak{a} \cap \mathfrak{q}^r) \subseteq \mathfrak{a} \cap \mathfrak{q}^{r+1}$ and therefore $(\mathfrak{a} \cap \mathfrak{q}^r)/(\mathfrak{a} \cap \mathfrak{q}^{r+1})$ is an A-module which is, moreover, finitely generated;† accordingly, by the above remarks,

$$\dim_A(\mathfrak{a} \cap \mathfrak{q}^r)/(\mathfrak{a} \cap \mathfrak{q}^{r+1})$$

is defined and is finite. By analogy with (1.2) we put

$$\chi_{\mathfrak{q}}(r, \mathfrak{a}) = \dim_A(\mathfrak{q}^r/\mathfrak{q}^{r+1}) - \dim_A(\mathfrak{a} \cap \mathfrak{q}^r)/(\mathfrak{a} \cap \mathfrak{q}^{r+1}) \tag{2.2}$$

and call $\chi_{\mathfrak{q}}(r, \mathfrak{a})$ the *Hilbert function* or *characteristic function* of $\mathfrak{a}$ with respect to $\mathfrak{q}$.

3. Elementary properties

We have, using $\cong$ to denote an isomorphism, the following isomorphisms between A-modules:

$$(\mathfrak{a}+\mathfrak{q}^r)/(\mathfrak{a}+\mathfrak{q}^{r+1}) \cong \mathfrak{q}^r/\mathfrak{q}^r \cap (\mathfrak{a}+\mathfrak{q}^{r+1}) \cong \mathfrak{q}^r/(\mathfrak{q}^r \cap \mathfrak{a}+\mathfrak{q}^{r+1}), \tag{3.1}$$

$$\mathfrak{q}^r/(\mathfrak{q}^r \cap \mathfrak{a}+\mathfrak{q}^{r+1}) \cong [\mathfrak{q}^r/\mathfrak{q}^{r+1}]/[(\mathfrak{q}^r \cap \mathfrak{a}+\mathfrak{q}^{r+1})/\mathfrak{q}^{r+1}], \tag{3.2}$$

$$(\mathfrak{q}^r \cap \mathfrak{a}+\mathfrak{q}^{r+1})/\mathfrak{q}^{r+1} \cong (\mathfrak{q}^r \cap \mathfrak{a})/(\mathfrak{q}^{r+1} \cap \mathfrak{a}). \tag{3.3}$$

From (3.1) and (3.2)

$$\dim_A(\mathfrak{a}+\mathfrak{q}^r)/(\mathfrak{a}+\mathfrak{q}^{r+1}) = \dim_A(\mathfrak{q}^r/\mathfrak{q}^{r+1}) - \dim_A(\mathfrak{q}^r \cap \mathfrak{a}+\mathfrak{q}^{r+1})/\mathfrak{q}^{r+1}$$

and from (3.3)

$$\dim_A(\mathfrak{q}^r \cap \mathfrak{a}+\mathfrak{q}^{r+1})/\mathfrak{q}^{r+1} = \dim_A(\mathfrak{q}^r \cap \mathfrak{a})/(\mathfrak{q}^{r+1} \cap \mathfrak{a}).$$

Hence by (2.2)
$$\chi_{\mathfrak{q}}(r, \mathfrak{a}) = \dim_A(\mathfrak{a}+\mathfrak{q}^r)/(\mathfrak{a}+\mathfrak{q}^{r+1}), \tag{3.4}$$

and therefore $\chi_{\mathfrak{q}}(r, \mathfrak{a})$ is the length of a composition series of ideals from $\mathfrak{a}+\mathfrak{q}^r$ to $\mathfrak{a}+\mathfrak{q}^{r+1}$. Now assume that $\mathfrak{a}$ is a proper ideal.‡ Put

$$\bar{Q} = Q/\mathfrak{a}, \qquad \bar{\mathfrak{q}} = (\mathfrak{a}+\mathfrak{q})/\mathfrak{a}.$$

Then $\bar{Q}$ is a local ring with maximal ideal $\bar{\mathfrak{m}} = \mathfrak{m}/\mathfrak{a}$ and $\bar{\mathfrak{q}}$ is an $\bar{\mathfrak{m}}$-primary ideal. Further, $\mathfrak{a}+\mathfrak{q}^r$ and $\bar{\mathfrak{q}}^r$ are corresponding ideals. This shows that the number of ideals in a composition series from $\mathfrak{a}+\mathfrak{q}^r$ to $\mathfrak{a}+\mathfrak{q}^{r+1}$ is the same as the number of ideals in a composition series from $\bar{\mathfrak{q}}^r$ to $\bar{\mathfrak{q}}^{r+1}$; and this latter is, in fact, $\chi_{\bar{\mathfrak{q}}}(r, \bar{O})$, where $\bar{O}$ is the zero ideal of $\bar{Q}$, as may be seen by taking $\mathfrak{a}$ to be zero ideal in (3.4). This proves

THEOREM 1. *Let $\mathfrak{a}$ be a proper ideal of Q, let $\bar{\mathfrak{q}} = (\mathfrak{a}+\mathfrak{q})/\mathfrak{a}$, and let $\bar{O}$ denote the zero ideal of $\bar{Q} = Q/\mathfrak{a}$. Then $\chi_{\mathfrak{q}}(r, \mathfrak{a}) = \chi_{\bar{\mathfrak{q}}}(r, \bar{O})$.*

COROLLARY 1. $\chi_{\mathfrak{q}}(r, \mathfrak{a}) = \chi_{\mathfrak{q}+\mathfrak{a}}(r, \mathfrak{a})$.

This follows from Theorem 1 immediately.

† By $\mathfrak{q}^0$ is meant Q itself.

‡ By a 'proper ideal' is meant an ideal which is not the whole ring.

COROLLARY 2. $\sum_{r=0}^{s-1} \chi_{\mathfrak{q}}(r, \mathfrak{a}) = P_{\bar{\mathfrak{q}}}(s)$ *where* $P_{\bar{\mathfrak{q}}}(s)$ *denotes the length of the primary ideal* $\bar{\mathfrak{q}}^s$.

Proof. We have seen that $\chi_{\mathfrak{q}}(r, \mathfrak{a})$ is equal to the length of a composition series of ideals from $\bar{\mathfrak{q}}^r$ to $\bar{\mathfrak{q}}^{r+1}$. The corollary follows by summation.

It is one of Samuel's basic results that $P_{\bar{\mathfrak{q}}}(s)$ is a polynomial in s for large values of s and that the degree of this polynomial is the dimension, $\dim \bar{Q}$, of $\bar{Q}$. More precisely, he proves [(**2**), Chapter 2, Theorems 1, 3] that there exists a non-negative integer s_0 such that, for all $s \geqslant s_0$,

$$P_{\bar{\mathfrak{q}}}(s) = a_0\binom{s}{l} + a_1\binom{s}{l-1} + \ldots + a_{l-1}\binom{s}{1} + a_l, \tag{3.5}$$

where the a_i are integers, where $a_0 > 0$, and where $l = \dim \bar{Q}$. The symbol $\binom{s}{r}$ denotes, of course, the familiar binomial coefficient. Since, by Corollary 2 of Theorem 1,

$$P_{\bar{\mathfrak{q}}}(s+1) - P_{\bar{\mathfrak{q}}}(s) = \chi_{\mathfrak{q}}(s, \mathfrak{a}) \tag{3.6}$$

we have, for all $s \geqslant s_0$,

$$\chi_{\mathfrak{q}}(s, \mathfrak{a}) = a_0\binom{s}{l-1} + a_1\binom{s}{l-2} + \ldots + a_{l+1} \quad (a_0 > 0), \tag{3.7}$$

$$l = \dim \mathfrak{a}. \tag{3.8}$$

Thus, for large s, $\chi_{\mathfrak{q}}(s, \mathfrak{a})$ is a polynomial in s of degree $\dim \mathfrak{a} - 1$. We call a_0 the *order of* $\mathfrak{a}$ *with respect to* $\mathfrak{q}$ and denote it by $\operatorname{ord}_{\mathfrak{q}} \mathfrak{a}$.

THEOREM 2. *Let* $\tilde{Q}$ *be the completion of* Q, *let* $\tilde{\mathfrak{a}} = \tilde{Q}\mathfrak{a}$, *and let* $\tilde{\mathfrak{q}} = \tilde{Q}\mathfrak{q}$. *Then* $\chi_{\mathfrak{q}}(r, \mathfrak{a}) = \chi_{\tilde{\mathfrak{q}}}(r, \tilde{\mathfrak{a}})$.

Proof. We have seen that $\chi_{\mathfrak{q}}(r, \mathfrak{a})$ is the length of a composition series of ideals from $\mathfrak{a}+\mathfrak{q}^r$ to $\mathfrak{a}+\mathfrak{q}^{r+1}$. In the same way $\chi_{\tilde{\mathfrak{q}}}(r, \tilde{\mathfrak{a}})$ is the length of a composition series from $\tilde{\mathfrak{a}}+\tilde{\mathfrak{q}}^r$ to $\tilde{\mathfrak{a}}+\tilde{\mathfrak{q}}^{r+1}$. Now, as is well known, if $\tilde{\mathfrak{m}}$ is the maximal ideal of $\tilde{Q}$, there is a 1–1 correspondence between the $\mathfrak{m}$-primary ideals $\mathfrak{q}'$ and the $\tilde{\mathfrak{m}}$-primary ideals $\tilde{\mathfrak{q}}'$ such that, if $\mathfrak{q}'$ and $\tilde{\mathfrak{q}}'$ correspond, then $\tilde{\mathfrak{q}}' = \tilde{Q}\mathfrak{q}'$ and $\mathfrak{q}' = \tilde{\mathfrak{q}}' \cap Q$. The theorem follows if we observe that $\tilde{Q}(\mathfrak{a}+\mathfrak{q}^r) = \tilde{\mathfrak{a}}+\tilde{\mathfrak{q}}^r$.

4. The form ideal

One method of developing the properties of $\chi_{\mathfrak{q}}(r, \mathfrak{a})$ is to introduce the so-called *form ideal* of $\mathfrak{a}$. We do this as follows. Let $\mathfrak{q} = (u_0, u_1, \ldots, u_n)$, where, however, this base of $\mathfrak{q}$ need not be minimal. Let $a \in Q$ $(a \neq 0)$; let $\phi(u) = \phi(u_0, u_1, \ldots, u_n)$ be a form of degree $s \geqslant 0$ in the u_i with coefficients in Q, and such that not all the coefficients of ϕ are in $\mathfrak{q}$;

further, let $\bar{\phi}(X) = \bar{\phi}(X_0, X_1, \ldots, X_n)$ be obtained from ϕ by replacing each u_i by an indeterminate X_i and each coefficient by its residue *modulo* $\mathfrak{q}$, thus making $\bar{\phi}(X)$ a form in the polynomial ring

$$A[X_0, X_1, \ldots, X_n].$$

If now $a \equiv \phi(u)\,(\mathfrak{q}^{s+1})$, the non-null form $\bar{\phi}(X)$ is called a *leading form* of a. The leading forms of the zero element are defined in exactly the same way except that we add to them the null form. If $a \neq 0$, then we can find s so that $a \in \mathfrak{q}^s$, $a \notin \mathfrak{q}^{s+1}$. It follows from this that each element of Q has at least one leading form.

Suppose next that $\mathfrak{a}$ is an arbitrary ideal in Q. The set of all leading forms of all elements of $\mathfrak{a}$ will generate a homogeneous ideal $\bar{\mathfrak{a}}$ in $A[X_0, X_1, \ldots, X_n]$, which will be termed the *form ideal*† of $\mathfrak{a}$. In the special case obtained by taking $\mathfrak{m} = \mathfrak{q}$ and choosing $(u_0, u_1, \ldots, u_n)$ to be a minimal base of $\mathfrak{m}$ the above defined form ideal is identical with the *Leitideal* of W. Krull [(**1**) 208]; and indeed, for reasons which will become clear shortly, Krull's investigations are of fundamental importance for the theory of the function $\chi_{\mathfrak{q}}(r, \mathfrak{a})$. Before we proceed, the reader should note that a simple consequence of the definition of the form ideal is that every form in $\bar{\mathfrak{a}}$ is a leading form of an element of $\mathfrak{a}$.

Denote by $\mathfrak{f}(r)$ the A-module consisting of all the forms of degree r in $A[X_0, X_1, \ldots, X_n]$ and denote by $\mathfrak{f}(r, \bar{\mathfrak{a}})$ the submodule composed of all the forms of degree r contained in $\bar{\mathfrak{a}}$. We put

$$\chi(r, \bar{\mathfrak{a}}) = \dim_A \mathfrak{f}(r) - \dim_A \mathfrak{f}(r, \bar{\mathfrak{a}}) \tag{4.1}$$

and call $\chi(r, \bar{\mathfrak{a}})$ the *Hilbert function* of the homogeneous ideal $\bar{\mathfrak{a}}$. Note that, if we compare (4.1) with (1.1), we see that, when $\mathfrak{q} = \mathfrak{m}$ (so that $A = Q/\mathfrak{m}$ is a field), $\chi(r, \bar{\mathfrak{a}})$ has its classical meaning. We come now to the key result, namely

THEOREM 3. *If $\bar{\mathfrak{a}}$ is the form ideal of $\mathfrak{a}$, then $\chi_{\mathfrak{q}}(r, \mathfrak{a}) = \chi(r, \bar{\mathfrak{a}})$.*

Proof. Let $\bar{\mathfrak{n}}$ be the form ideal of the zero ideal in Q and let $r \geqslant 0$ be a fixed integer. If $a \in \mathfrak{a} \cap \mathfrak{q}^r$, then we can find at least one form ϕ of degree r such that $a \equiv \phi(u)\,(\mathfrak{q}^{r+1})$. We now have $\bar{\phi}(X) \in \bar{\mathfrak{a}}$, because either $\bar{\phi}(X)$ is not null and therefore it is a leading form of a, or else it is null and the assertion is trivial. Thus $\bar{\phi}(X) \in \mathfrak{f}(r, \bar{\mathfrak{a}})$ and it is easily verified that all elements of $\mathfrak{f}(r, \bar{\mathfrak{a}})$ arise in this way. Further, if ϕ_1 is a second such form, i.e. if

$$a \equiv \phi(u) \equiv \phi_1(u)\,(\mathfrak{q}^{r+1}),$$

† The base $(u_0, u_1, \ldots, u_n)$ will be kept fixed. On this understanding form ideals are uniquely determined.

then $\bar{\phi}(X)-\bar{\phi}_1(X)$ is a leading form of the zero element and therefore $\bar{\phi}(X) \equiv \bar{\phi}_1(X)$ *modulo* $\mathfrak{f}(r, \bar{\mathfrak{n}})$. Consider the mapping

$$a \to \bar{\phi}+\mathfrak{f}(r, \bar{\mathfrak{n}}).$$

It is a single-valued mapping of $\mathfrak{a} \cap \mathfrak{q}^r$ on to $\mathfrak{f}(r, \bar{\mathfrak{a}})/\mathfrak{f}(r, \bar{\mathfrak{n}})$ which, as is easily verified, preserves addition. The element $a \in \mathfrak{a} \cap \mathfrak{q}^r$ will be mapped into zero if and only if $\bar{\phi} \in \bar{\mathfrak{n}}$, and this will happen if and only if

$$0 \equiv \phi(u)\,(\mathfrak{q}^{r+1}).$$

But $a \equiv \phi(u)\,(\mathfrak{q}^{r+1})$ and so we see that a is mapped into zero if and only if $a \in \mathfrak{a} \cap \mathfrak{q}^{r+1}$. Thus $(\mathfrak{a} \cap \mathfrak{q}^r)/(\mathfrak{a} \cap \mathfrak{q}^{r+1})$ and $\mathfrak{f}(r, \bar{\mathfrak{a}})/\mathfrak{f}(r, \bar{\mathfrak{n}})$ are certainly isomorphic as additive groups, and now it is easily verified that the isomorphism is preserved if we regard them as A-modules. It follows that

$$\dim_A(\mathfrak{a} \cap \mathfrak{q}^r)/(\mathfrak{a} \cap \mathfrak{q}^{r+1}) = \dim_A \mathfrak{f}(r, \bar{\mathfrak{a}})-\dim_A \mathfrak{f}(r, \bar{\mathfrak{n}}), \tag{B}$$

which includes

$$\dim_A \mathfrak{q}^r/\mathfrak{q}^{r+1} = \dim_A \mathfrak{f}(r)-\dim_A \mathfrak{f}(r, \bar{\mathfrak{n}}), \tag{C}$$

as may be seen by taking $\mathfrak{a} = (1)$. The theorem is obtained by subtracting (B) from (C).

5. Hilbert functions in the ring $A[X_0, X_1, \ldots, X_n]$

After Theorem 3, it is convenient to continue the discussion of the function $\chi_0(r, \mathfrak{a})$ in two stages. The first stage, which will be considered in the present section, concerns the theory of Hilbert functions of homogeneous ideals in $A[X_0, X_1, \ldots, X_n]$. We shall find that, at least in so far as the more elementary results are concerned, the classical theory is unaffected by changing the coefficients from field elements to the elements of a primary ring. This observation may be said to form the starting point of Samuel's thesis, but, for the applications to be made here, we must elaborate the idea behind the observation in greater detail. This elaboration will be achieved by adapting the elegant exposition of the classical theory given by B. L. van der Waerden [(**3**) 511–13].

Throughout the remainder of § 5, $\bar{\mathfrak{a}}$, $\bar{\mathfrak{b}}$, etc., will denote homogeneous ideals in $A[X_0, X_1, \ldots, X_n]$, which need not be form ideals of ideals in Q. The Hilbert function of a general homogeneous ideal $\bar{\mathfrak{a}}$ is to be defined by means of (4.1). Since $\bar{\mathfrak{a}}$ and $\bar{\mathfrak{b}}$ are homogeneous, we have

$$\mathfrak{f}(r, \bar{\mathfrak{a}}+\bar{\mathfrak{b}}) = \mathfrak{f}(r, \bar{\mathfrak{a}})+\mathfrak{f}(r, \bar{\mathfrak{b}}) \quad \text{and} \quad \mathfrak{f}(r, \bar{\mathfrak{a}} \cap \bar{\mathfrak{b}}) = \mathfrak{f}(r, \bar{\mathfrak{a}}) \cap \mathfrak{f}(r, \bar{\mathfrak{b}}).$$

Consequently, by (2.1),

$$\dim_A \mathfrak{f}(r, \bar{\mathfrak{a}}+\bar{\mathfrak{b}})+\dim_A \mathfrak{f}(r, \bar{\mathfrak{a}} \cap \bar{\mathfrak{b}}) = \dim_A \mathfrak{f}(r, \bar{\mathfrak{a}})+\dim_A \mathfrak{f}(r, \bar{\mathfrak{b}}),$$

from which it follows at once that

$$\chi(r,\bar{\mathfrak{a}}+\bar{\mathfrak{b}})+\chi(r,\bar{\mathfrak{a}}\cap\bar{\mathfrak{b}})=\chi(r,\bar{\mathfrak{a}})+\chi(r,\bar{\mathfrak{b}}). \tag{5.1}$$

Let us now recall the special nature of the ring A. $A=Q/\mathfrak{q}$ is a primary ring and $\mathfrak{p}=\mathfrak{m}/\mathfrak{q}$ is its single prime ideal. Let $\bar{\mathfrak{p}}$ be the extension of $\mathfrak{p}$ in $A[X_0,X_1,\ldots,X_n]$; then, since $\mathfrak{p}$ is the only prime ideal belonging to the zero ideal of A, $\bar{\mathfrak{p}}$ is prime and it is the only prime ideal belonging to the zero ideal of $A[X_0,X_1,\ldots,X_n]$. Two useful consequences of this observation are stated in

LEMMA 1. *Every prime ideal in $A[X_0,X_1,\ldots,X_n]$ contains $\bar{\mathfrak{p}}$. If $\bar{\phi}(X)$ does not belong to $\bar{\mathfrak{p}}$, then $\bar{\phi}(X)$ is not a zero divisor in $A[X_0,X_1,\ldots,X_n]$.*

THEOREM 4. *Let $\bar{\mathfrak{a}}$ be a homogeneous ideal and let $\bar{\phi}(X)$ be a form of degree l such that $\bar{\mathfrak{a}}:(\bar{\phi})=\bar{\mathfrak{a}}$. Then*

$$\chi[r,\bar{\mathfrak{a}}+(\bar{\phi})]=\chi(r,\bar{\mathfrak{a}})-\chi(r-l,\bar{\mathfrak{a}})$$

for $r\geqslant l$, while $\chi[r,\bar{\mathfrak{a}}+(\bar{\phi})]=\chi(r,\bar{\mathfrak{a}})$ for $0\leqslant r<l$.

Proof. We may assume that $\bar{\mathfrak{a}}\neq(1)$. Since $\bar{\mathfrak{a}}:(\bar{\phi})=\bar{\mathfrak{a}}$, $\bar{\phi}$ is not contained in any prime ideal of $\bar{\mathfrak{a}}$ and therefore, *a fortiori*, $\bar{\phi}\notin\bar{\mathfrak{p}}$ (see Lemma 1). This shows that $\bar{\phi}$ is not a zero divisor. For $r\geqslant l$ we have, as is easily verified,

$$\mathfrak{f}[r,\bar{\mathfrak{a}}\cap(\bar{\phi})]=\bar{\phi}\mathfrak{f}[r-l,\bar{\mathfrak{a}}] \quad\text{and}\quad \mathfrak{f}[r,(\bar{\phi})]=\bar{\phi}\mathfrak{f}[r-l].$$

Consequently, since $\bar{\phi}$ is not a zero divisor,

$$\mathfrak{f}[r,\bar{\mathfrak{a}}\cap(\bar{\phi})]\cong\mathfrak{f}[r-l,\bar{\mathfrak{a}}] \quad\text{and}\quad \mathfrak{f}[r,(\bar{\phi})]\cong\mathfrak{f}[r-l],$$

where in the two isomorphisms all the terms are to be regarded as A-modules. In particular we have

$$\begin{aligned}\dim_A\mathfrak{f}[r,(\bar{\phi})]-\dim_A\mathfrak{f}[r,\bar{\mathfrak{a}}\cap(\bar{\phi})]&=\dim_A\mathfrak{f}[r-l]-\dim_A\mathfrak{f}[r-l,\bar{\mathfrak{a}}]\\&=\chi[r-l,\bar{\mathfrak{a}}]\end{aligned} \tag{D}$$

for $r\geqslant l$. Again, by (5.1) and the definition of the Hilbert function, we have for any $r\geqslant 0$

$$\chi[r,\bar{\mathfrak{a}}+(\bar{\phi})]=\chi[r,\bar{\mathfrak{a}}]+\dim_A\mathfrak{f}[r,\bar{\mathfrak{a}}\cap(\bar{\phi})]-\dim_A\mathfrak{f}[r,(\bar{\phi})],$$

which is equal to $\chi[r,\bar{\mathfrak{a}}]-\chi[r-l,\bar{\mathfrak{a}}]$ by (D) if $r\geqslant l$, but which reduces to $\chi[r,\bar{\mathfrak{a}}]$ if $r<l$. This completes the proof.

Note. For future reference we observe that the conclusion of Theorem 4 can be put in the following form. The value of $\chi[r,\bar{\mathfrak{a}}+(\bar{\phi})]$ is, for all $r\geqslant 0$, equal to the coefficient of x^r in $(1-x^l)\sum_{\nu=0}^{\infty}\chi(\nu,\bar{\mathfrak{a}})x^\nu$.

Let $\mathfrak{X}=(\bar{\mathfrak{p}},X_0,X_1,\ldots,X_n)$; then $\mathfrak{X}$ is a maximal prime ideal in $A[X_0,X_1,\ldots,X_n]$ and it contains every proper homogeneous ideal. $\mathfrak{X}$ takes over the role played by $(X_0,X_1,\ldots,X_n)$ in the classical theory.

LEMMA 2. *Suppose that a proper homogeneous ideal* $\bar{\mathfrak{a}}$ *contains a power of* $(X_0, X_1, \ldots, X_n)$. *Then* $\bar{\mathfrak{a}}$ *is* $\mathfrak{X}$*-primary.*

Proof. Suppose that $(X_0, X_1, \ldots, X_n)^r \subseteq \bar{\mathfrak{a}}$. Since $\bar{\mathfrak{p}}$ is the only prime ideal belonging to the zero ideal, we can find an integer s such that $\bar{\mathfrak{p}}^s = (0)$, and then $\mathfrak{X}^s = (\bar{\mathfrak{p}}, X_0, X_1, \ldots, X_n)^s$ is contained in $(X_0, X_1, \ldots, X_n)$. Consequently $\mathfrak{X}^{rs} \subseteq \bar{\mathfrak{a}}$, and now the lemma follows.

LEMMA 3. *Let* $\bar{\mathfrak{a}}$ *be a proper homogeneous ideal. If* $\bar{\mathfrak{a}}$ *is of dimension zero, then* $\chi(r, \bar{\mathfrak{a}}) = 0$ *for all sufficiently large values of* r. *If, however,* $\bar{\mathfrak{a}}$ *is of strictly positive dimension, then* $\chi(r, \bar{\mathfrak{a}}) > 0$ *for all* r.†

Proof. First assume that the dimension $\dim \bar{\mathfrak{a}}$ of $\bar{\mathfrak{a}}$ is zero. This means that $\bar{\mathfrak{a}}$ is $\mathfrak{X}$-primary; consequently we can find s so that

$$(X_0, X_1, \ldots, X_n)^s \subseteq \mathfrak{X}^s \subseteq \bar{\mathfrak{a}}$$

and then, for $r \geqslant s$, we have $\mathfrak{f}(r) = \mathfrak{f}(r, \bar{\mathfrak{a}})$ and therefore $\chi(r, \bar{\mathfrak{a}}) = 0$. Now assume that $\dim \bar{\mathfrak{a}} > 0$ and let $r \geqslant 0$ be an arbitrary integer. Since $\bar{\mathfrak{a}}$ cannot be $\mathfrak{X}$-primary, we see, by Lemma 2, that $(X_0, X_1, \ldots, X_n)^r$ cannot be contained in $\bar{\mathfrak{a}}$. Consequently $\mathfrak{f}(r) \supset \mathfrak{f}(r, \bar{\mathfrak{a}})$, where the inclusion is strict. It follows that

$$\chi(r, \bar{\mathfrak{a}}) = \dim_A \mathfrak{f}(r) - \dim_A \mathfrak{f}(r, \bar{\mathfrak{a}}) > 0,$$

as required.

THEOREM 5. *If* $\bar{\mathfrak{a}}$ *is a homogeneous ideal of dimension* $d \geqslant 0$, *then there exist integers* $a_0, a_1, a_2, \ldots, a_{d-1}$ *such that*

$$\chi(r, \bar{\mathfrak{a}}) = a_0 \binom{r}{d-1} + a_1 \binom{r}{d-2} + \ldots + a_{d-1} \quad (a_0 \geqslant 0)$$

for all sufficiently large values of r.

Note. If $d = 0$, the theorem must be regarded as asserting that $\chi(r, \bar{\mathfrak{a}}) = 0$ for all large values of r. It will be proved subsequently that, for ideals of strictly positive dimension, a_0 is always definitely greater than zero.

Proof. If $d = 0$, the theorem has already been proved (Lemma 3). We assume therefore that $d > 0$ and we assume also that the theorem has been proved for homogeneous ideals of smaller dimensions. Suppose first that $\bar{\mathfrak{a}}$ is primary and let it be $\bar{\mathfrak{p}}_1$-primary. Then $\bar{\mathfrak{p}}_1 \not\supseteq (X_0, X_1, \ldots, X_n)$, for otherwise, by Lemma 2, $\bar{\mathfrak{p}}_1$ would be the same as $\mathfrak{X}$ contrary to the hypothesis $d > 0$. Choose j so that $X_j \notin \bar{\mathfrak{p}}_1$; then $\bar{\mathfrak{a}} : (X_j) = \bar{\mathfrak{a}}$, so that, by Theorem 4,

$$\chi[r, \bar{\mathfrak{a}} + (X_j)] = \chi(r, \bar{\mathfrak{a}}) - \chi(r-1, \bar{\mathfrak{a}})$$

† By the 'dimension' of $\bar{\mathfrak{a}}$ we mean the ordinary and not the projective dimension. For example, $\mathfrak{X}$ has dimension zero.

for $r \geqslant 1$. Now $\bar{\mathfrak{a}}+(X_j)$ has dimension less than d. Consequently, by the inductive hypothesis, we can find integers $b_0, b_1, \ldots, b_{d-2}$ $(b_0 \geqslant 0)$ such that

$$\chi(r, \bar{\mathfrak{a}})-\chi(r-1, \bar{\mathfrak{a}}) = b_0\binom{r}{d-2}+b_1\binom{r}{d-3}+\ldots+b_{d-2}$$

for all $r \geqslant r_0$ (say). By summation we obtain

$$\chi(r, \bar{\mathfrak{a}})-\chi(r_0, \bar{\mathfrak{a}}) = b_0\left[\binom{r+1}{d-1}-\binom{r_0+1}{d-1}\right]+$$

$$+b_1\left[\binom{r+1}{d-2}-\binom{r_0+1}{d-2}\right]+\ldots+b_{d-2}\left[\binom{r+1}{1}-\binom{r_0+1}{1}\right],$$

i.e. $$\chi(r, \bar{\mathfrak{a}}) = c_0\binom{r+1}{d-1}+c_1\binom{r+1}{d-2}+\ldots+c_{d-1} \quad (c_0 \geqslant 0)$$

for all $r \geqslant r_0$, where the c_i are integers. If we replace

$$\binom{r+1}{d-1} \text{ by } \binom{r}{d-1}+\binom{r}{d-2}, \qquad \binom{r+1}{d-2} \text{ by } \binom{r}{d-2}+\binom{r}{d-3},$$

and so on and then regroup the terms, we obtain an expression for $\chi(r, \bar{\mathfrak{a}})$ of the required form.

Let us now remove the restriction that $\bar{\mathfrak{a}}$ must be primary. In the general case $\bar{\mathfrak{a}}$ will have a reduced primary decomposition, say

$$\bar{\mathfrak{a}} = \bar{\mathfrak{q}}_1 \cap \bar{\mathfrak{q}}_2 \cap \ldots \cap \bar{\mathfrak{q}}_l = \bar{\mathfrak{b}} \cap \bar{\mathfrak{q}}_l,$$

where the $\bar{\mathfrak{q}}_i$ are homogeneous primary ideals, and where we may suppose that $\bar{\mathfrak{q}}_l$ has dimension d. If $l = 1$, the theorem is proved. We assume therefore that $l > 1$ and that the theorem holds for d-dimensional ideals with fewer than l primary components. Let us observe that

$$\chi(r, \bar{\mathfrak{a}}) = \chi(r, \bar{\mathfrak{q}}_l)+\chi(r, \bar{\mathfrak{b}})-\chi(r, \bar{\mathfrak{q}}_l+\bar{\mathfrak{b}})$$

and let us consider, in turn, the terms on the right-hand side. By what has just been proved, the first of these has the required form. In considering $\chi(r, \bar{\mathfrak{b}})$ we distinguish two cases. Either $\dim \bar{\mathfrak{b}} = d$, in which case (since $\bar{\mathfrak{b}}$ has fewer than l primary components) $\chi(r, \bar{\mathfrak{b}})$ has the required form by the second inductive hypothesis; or else $\dim \bar{\mathfrak{b}} < d$, and again $\chi(r, \bar{\mathfrak{b}})$ can be written in the form

$$A_0\binom{r}{d-1}+A_1\binom{r}{d-2}+\ldots+A_{d-1}, \qquad \text{(E)}$$

but this time the coefficient A_0 will be zero. Finally, the dimension of $\bar{\mathfrak{q}}_l+\bar{\mathfrak{b}}$ is definitely less than d; consequently we can write $\chi(r, \bar{\mathfrak{q}}_l+\bar{\mathfrak{b}})$ in

the form (E) by taking the coefficient of $\binom{r}{d-1}$ to be zero. The theorem follows by combining these remarks.

DEFINITION. *If $\bar{\mathfrak{a}}$ is homogeneous and d-dimensional then the coefficient a_0 of $\binom{r}{d-1}$ in the expression for $\chi(r, \bar{\mathfrak{a}})$ will be called the 'order' of $\bar{\mathfrak{a}}$ and it will be denoted by* $\operatorname{ord} \bar{\mathfrak{a}}$.

Let $\bar{\mathfrak{q}}_1, \bar{\mathfrak{q}}_2, \ldots, \bar{\mathfrak{q}}_p$ be the uniquely-determined d-dimensional primary components of a d-dimensional homogeneous ideal $\bar{\mathfrak{a}}$; then the method of proof of Theorem 5 shows that

$$\operatorname{ord} \bar{\mathfrak{a}} = \operatorname{ord} \bar{\mathfrak{q}}_1 + \operatorname{ord} \bar{\mathfrak{q}}_2 + \ldots + \operatorname{ord} \bar{\mathfrak{q}}_p. \tag{5.2}$$

THEOREM 6. *If $\bar{\mathfrak{a}}$ is homogeneous and of dimension $d > 0$, then* $\operatorname{ord} \bar{\mathfrak{a}} > 0$ *and $\chi(r, \bar{\mathfrak{a}})$ is, for large r, a polynomial in r of which the degree is exactly $d-1$.*

Proof. Assume, first, that $d = 1$. Then $\chi(r, \bar{\mathfrak{a}}) = \operatorname{ord} \bar{\mathfrak{a}}$ for all large r. By Lemma 3, $\chi(r, \bar{\mathfrak{a}}) > 0$ for all r. Consequently $\operatorname{ord} \bar{\mathfrak{a}} > 0$. This shows that we may assume that $d > 1$ and we may also assume that the theorem holds for ideals which have dimension $d-1$. Further, by (5.2), we may confine ourselves to the case where $\mathfrak{a}$ is primary; let it be $\bar{\mathfrak{p}}_1$-primary, where $\dim \bar{\mathfrak{p}}_1 = d > 1$. By Lemma 2, $(X_0, X_1, \ldots, X_n)$ is not contained in $\bar{\mathfrak{p}}_1$; accordingly we can choose j so that $X_j \notin \bar{\mathfrak{p}}_1$, and then we shall have (see Theorem 4)

$$\chi[r, \bar{\mathfrak{a}} + (X_j)] = \chi(r, \bar{\mathfrak{a}}) - \chi(r-1, \bar{\mathfrak{a}}) = \frac{\operatorname{ord} \bar{\mathfrak{a}}}{(d-2)!} r^{d-2} + \ldots .$$

If, therefore, we show that $\bar{\mathfrak{a}} + (X_j)$ is of dimension $d-1$, it will follow from the inductive hypothesis that $\operatorname{ord} \bar{\mathfrak{a}} > 0$, and this will complete the proof. Now the prime ideals which contain $\bar{\mathfrak{a}} + (X_j)$ are the same as the prime ideals which contain $\bar{\mathfrak{p}}_1 + (X_j)$. Consequently it is enough to show that $\bar{\mathfrak{p}}_1 + (X_j)$ has dimension $d-1$. By Lemma 1, $\bar{\mathfrak{p}} \subseteq \bar{\mathfrak{p}}_1$, where, as before, $\bar{\mathfrak{p}}$ denotes the unique minimal prime ideal of $A[X_0, X_1, \ldots, X_n]$. As is easily verified, $A[X_0, X_1, \ldots, X_n]/\bar{\mathfrak{p}}$ can be identified with

$$K[X_0, X_1, \ldots, X_n],$$

where K is the field $A/\mathfrak{p}$ and where X_i corresponds to itself. In

$$K[X_0, X_1, \ldots, X_n],$$

$\bar{\mathfrak{p}}_1/\bar{\mathfrak{p}}$ is a homogeneous d-dimensional prime ideal which does not contain X_j and we wish to show that $\bar{\mathfrak{p}}_1/\bar{\mathfrak{p}} + (X_j)$ is $(d-1)$-dimensional. This, however, follows by well-known properties of ordinary polynomial rings.

6. Applications to the general theory

By combining Theorems 3, 5, 6 with (3.7) and (3.8) we obtain the following generalization of a theorem of Krull's [(**1**) Theorem 8, 210]:

THEOREM 7. *If* $\mathfrak{a}$ *is an ideal in* Q *and if* $\bar{\mathfrak{a}}$ *is its form ideal, then* $\mathfrak{a}$ *and* $\bar{\mathfrak{a}}$ *have the same dimension and they have the same order;* $\operatorname{ord}_{\mathfrak{q}} \mathfrak{a} = \operatorname{ord} \bar{\mathfrak{a}}$.

Suppose that $\mathfrak{a}$ is a d-dimensional ideal in Q. Let $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_r$ be the uniquely-determined primary components belonging to the d-dimensional prime ideals of $\mathfrak{a}$; then we shall call $\mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \ldots \cap \mathfrak{q}_r$ the *d-dimensional component of* $\mathfrak{a}$. The d-dimensional component of a d-dimensional ideal in $A[X_0, X_1, \ldots, X_n]$ is defined in the same way. If $\mathfrak{a}_0$ is the d-dimensional component of $\mathfrak{a}$, we have $\mathfrak{a}_0 \supseteq \mathfrak{a} = \mathfrak{a}_0 \cap \mathfrak{b}$, where $\dim \mathfrak{b} < d$, and from this follows $\bar{\mathfrak{a}}_0 \supseteq \bar{\mathfrak{a}} \supseteq \bar{\mathfrak{a}}_0 \bar{\mathfrak{b}}$, where $\bar{\mathfrak{a}}$, $\bar{\mathfrak{b}}$, and $\bar{\mathfrak{a}}_0$ are the form ideals of $\mathfrak{a}$, $\mathfrak{b}$, and $\mathfrak{a}_0$. By Theorem 7, $\dim \bar{\mathfrak{a}}_0 = \dim \bar{\mathfrak{a}} = d$ and $\dim \bar{\mathfrak{b}} < d$, and it is now an easy matter to show that $\bar{\mathfrak{a}}_0$ and $\bar{\mathfrak{a}}$ have the same d-dimensional component. By (5.2), it follows that $\operatorname{ord} \bar{\mathfrak{a}}_0 = \operatorname{ord} \bar{\mathfrak{a}}$, hence (Theorem 7) $\operatorname{ord}_{\mathfrak{q}} \mathfrak{a} = \operatorname{ord}_{\mathfrak{q}} \mathfrak{a}_0$, which shows that $\operatorname{ord}_{\mathfrak{q}} \mathfrak{a}$ depends only on the d-dimensional component of $\mathfrak{a}$. Thus we have

THEOREM 8. *If* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are* d*-dimensional ideals in* Q *and if they have the same* d*-dimensional component, then* $\operatorname{ord}_{\mathfrak{q}} \mathfrak{a} = \operatorname{ord}_{\mathfrak{q}} \mathfrak{b}$.

THEOREM 9. *Let* $\mathfrak{a}$ *be an ideal of* Q *and suppose that the element* $c \in Q$ *has a leading form* $\bar{\phi}$ *such that* $\bar{\mathfrak{a}} : (\bar{\phi}) = \bar{\mathfrak{a}}$. *Then* $\overline{(\mathfrak{a}, c)} = (\bar{\mathfrak{a}}, \bar{\phi})$.

This theorem is a slight generalization of one due to Krull [(**1**) Theorem 12, 212]. The proof given is that given by Krull.

Let $\bar{\phi}$ be of degree l and let ϕ be obtained from $\bar{\phi}$ by replacing each coefficient of $\bar{\phi}$ by one of its representatives. Then it is clear that we can choose these representatives so as to make $c = \phi(u)$. I shall now establish

LEMMA 4. *For* $\mu = 0, 1, 2, \ldots$ *we have*

$$(\mathfrak{a} + \mathfrak{q}^{l+\mu}) : (c) \subseteq \mathfrak{a} + \mathfrak{q}^{\mu}.$$

Proof. The assertion is trivial for $\mu = 0$. We may therefore suppose that $\mu > 0$ and also that $(\mathfrak{a} + \mathfrak{q}^{l+\mu-1}) : (c) \subseteq \mathfrak{a} + \mathfrak{q}^{\mu-1}$.

Let $x \in (\mathfrak{a} + \mathfrak{q}^{l+\mu}) : (c)$. Then, *a fortiori*,

$$x \in (\mathfrak{a} + \mathfrak{q}^{l+\mu-1}) : (c) \subseteq \mathfrak{a} + \mathfrak{q}^{\mu-1},$$

so that $x = a + y$, where $a \in \mathfrak{a}$ and $y = \psi(u)$, where ψ is a form of degree $\mu - 1$. Thus

$$ca + cy = cx \in \mathfrak{a} + \mathfrak{q}^{\mu+l}$$

and therefore

$$ca + a_1 + cy \in \mathfrak{q}^{\mu+l}$$

for a suitable $a_1 \in \mathfrak{a}$. Now $c \in \mathfrak{q}^l$; hence $ca+a_1 \in \mathfrak{q}^{\mu+l-1}$, say $ca+a_1 = \omega(u)$, where ω is a form of degree $\mu+l-1$. We now have

$$\omega(u)+\phi(u)\psi(u) \equiv 0\,(\mathfrak{q}^{\mu+l}),$$

which shows that $\bar{\omega}+\bar{\phi}\bar{\psi}$ is a leading form of the zero element and therefore (weakening the assertion) $\bar{\omega}+\bar{\phi}\bar{\psi} \in \bar{\mathfrak{a}}$. But, by construction, $\bar{\omega} \in \bar{\mathfrak{a}}$; accordingly $\bar{\psi} \in \bar{\mathfrak{a}}\colon(\bar{\phi}) = \bar{\mathfrak{a}}$, which shows that we can find $a_2 \in \mathfrak{a}$ such that $a_2 \equiv \psi(u) = y(\mathfrak{q}^{\mu})$. Thus

$$x = a+y = (a+a_2)+(y-a_2) \in \mathfrak{a}+\mathfrak{q}^{\mu},$$

as required.

Proof of Theorem 9. It is clear that $(\bar{\mathfrak{a}}, \bar{\phi}) \subseteq \overline{(\mathfrak{a}, c)}$. Let $b = a+rc$ where $a \in \mathfrak{a}$ and $r \in Q$. It is sufficient to prove that all the leading forms of b are in $(\bar{\mathfrak{a}}, \bar{\phi})$, and therefore we may suppose that $b \neq 0$. Choose h so that $b \in \mathfrak{q}^h$, $b \notin \mathfrak{q}^{h+1}$. If $h < l$, then

$$a \in \mathfrak{q}^h, \qquad a \notin \mathfrak{q}^{h+1}, \qquad a \equiv b\,(\mathfrak{q}^{h+1})$$

and it follows that b and a have the same leading forms, which will necessarily be in $\bar{\mathfrak{a}} \subseteq (\bar{\mathfrak{a}}, \bar{\phi})$. We may therefore suppose, in what follows, that $h = l+\mu$, where $\mu \geqslant 0$. We now have $r \in (\mathfrak{a}+\mathfrak{q}^{l+\mu})\colon(c)$. Consequently, by Lemma 4, $r = a_1+z$, where $a_1 \in \mathfrak{a}$ and $z \in \mathfrak{q}^{\mu}$, say $z = \psi(u)$, where ψ is a form of degree μ. Again $b = a+ca_1+\phi(u)\psi(u)$; consequently $a+ca_1 \in \mathfrak{q}^{\mu+l}$, say $a+ca_1 = \omega(u)$, where ω is a form of degree $\mu+l$. Thus

$$b = \omega(u)+\phi(u)\psi(u) = \pi(u),$$

where π is the form $\omega+\phi\psi$ which is of degree $\mu+l$. Before proceeding, note that $\bar{\pi} = \bar{\omega}+\bar{\phi}\bar{\psi} \in (\bar{\mathfrak{a}}, \bar{\phi})$ because, by construction, $\bar{\omega} \in \bar{\mathfrak{a}}$. Let $\bar{\pi}_1$ be an arbitrary leading form of b and let its degree be s. Then $b \in \mathfrak{q}^s$ and consequently $s \leqslant l+\mu$. If $s < \mu+l$, then, since $b \equiv \pi_1(u)\,(\mathfrak{q}^{s+1})$ and $b \equiv 0\,(\mathfrak{q}^{s+1})$, $\bar{\pi}_1$ is a leading form of the zero element, and for trivial reasons $\bar{\pi}_1$ belongs to $(\bar{\mathfrak{a}}, \bar{\phi})$. If $s = \mu+l$, then $\pi(u) = b \equiv \pi_1(u)\,(\mathfrak{q}^{\mu+l+1})$, which shows that $\bar{\pi}-\bar{\pi}_1$ is a leading form of the zero element and therefore $\bar{\pi}_1-\bar{\pi} \in (\bar{\mathfrak{a}}, \bar{\phi})$. But it has already been shown that $\bar{\pi} \in (\bar{\mathfrak{a}}, \bar{\phi})$. Consequently $\bar{\pi}_1 \in (\bar{\mathfrak{a}}, \bar{\phi})$ as required.

THEOREM 10. *Let $\mathfrak{a}$ be a proper ideal of Q and let c be an element which has a leading form $\bar{\phi}$ satisfying $\bar{\mathfrak{a}}\colon(\bar{\phi}) = \bar{\mathfrak{a}}$, where $\bar{\mathfrak{a}}$ is the form ideal of $\mathfrak{a}$. Then, for $r \geqslant l$,*

$$\chi_{\mathfrak{q}}[r, (\mathfrak{a}, c)] = \chi_{\mathfrak{q}}[r, \mathfrak{a}]-\chi_{\mathfrak{q}}[r-l, \mathfrak{a}],$$

where l is defined by $c \in \mathfrak{q}^l$, $c \notin \mathfrak{q}^{l+1}$.

Proof. By Theorems 3 and 9,

$$\chi_{\mathfrak{q}}[r, (\mathfrak{a}, c)] = \chi[r, \overline{(\mathfrak{a}, c)}] = \chi[r, (\bar{\mathfrak{a}}, \bar{\phi})].$$

Consequently, by Theorems 3 and 4,

$$\chi_{\mathfrak{q}}[r,(a,c)] = \chi[r,\bar{\mathfrak{a}}]-\chi[r-\lambda,\bar{\mathfrak{a}}]$$
$$= \chi_{\mathfrak{q}}[r,\mathfrak{a}]-\chi_{\mathfrak{q}}[r-\lambda,\bar{\mathfrak{a}}],$$

where λ is the degree of $\bar{\phi}$. It remains for me to show that $\lambda = l$. Now, with the usual notations, $c \equiv \phi(u)\ (\mathfrak{q}^{\lambda+1})$. Hence $c \in \mathfrak{q}^{\lambda}$ and therefore $\lambda \leqslant l$. But λ cannot be less than l. For, if $\lambda < l$, then $0 \equiv \phi(u)\ (\mathfrak{q}^{\lambda+1})$ and so $\bar{\phi}$ is a leading form of the zero element, which implies that $\bar{\phi} \in \bar{\mathfrak{a}}$. This, however, contradicts $\bar{\mathfrak{a}}:(\bar{\phi}) = \bar{\mathfrak{a}}$.

7. A special example

In order to illustrate the general theory, I shall consider the case in which Q is a regular local ring and $\mathfrak{q} = \mathfrak{m}$, the maximal ideal. We suppose, too, that $(u_0, u_1, u_2, \ldots, u_n)$ is a *minimal* base of $\mathfrak{m}$, so that, since Q is regular, we have $m = n+1$, where m is the dimension of Q. Again, it follows from the definition of regularity that each element $a \in Q$ has a *unique* leading form; we shall denote it by $\bar{a}$. This is convenient because we then have $\overline{(a)} = (\bar{a})$. Note that, since $\mathfrak{q} = \mathfrak{m}$, we have another simplification: namely $A[X_0, X_1, \ldots, X_n]$ is an ordinary polynomial ring where the coefficients are in a field.

THEOREM 11. *Let Q be a regular local ring of dimension m and let $a_1, a_2, \ldots, a_s$ $(s < m)$ be elements of Q such that $(\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_s)$ is an ideal of rank s. Let l_i be defined by $a_i \in \mathfrak{m}^{l_i}$, $a_i \notin \mathfrak{m}^{l_i+1}$. Then $\chi_{\mathfrak{m}}[r,(a_1,a_2,\ldots,a_s)]$ is the coefficient of x^r in $(1-x^{l_1})(1-x^{l_2})\ldots(1-x^{l_s})(1-x)^{-m}$ and*

$$\operatorname{ord}_{\mathfrak{m}}(a_1,a_2,\ldots,a_s) = l_1 l_2 \ldots l_s.$$

Proof. The $\bar{a}_j$ are forms in $K[X_0, X_1, \ldots, X_n]$, where K is the field $Q/\mathfrak{m}$, and $\bar{a}_j$ is of degree l_j. Further (for each j satisfying $1 \leqslant j \leqslant s$)

$$\operatorname{rank}(\bar{a}_1,\bar{a}_2,\ldots,\bar{a}_j) \leqslant j.$$

But, since we are dealing with proper homogeneous ideals,

$$\operatorname{rank}(\bar{a}_1,\bar{a}_2,\ldots,\bar{a}_j,\bar{a}_{j+1}) \leqslant 1+\operatorname{rank}(\bar{a}_1,\bar{a}_2,\ldots,\bar{a}_j).$$

In fact, if $\bar{\mathfrak{p}}_1$ is a prime ideal of $(\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_j)$, it will be proper and homogeneous, and therefore $\bar{\mathfrak{p}}_1+(\bar{a}_{j+1})$ will be contained in $(X_0, X_1, \ldots, X_n)$. It follows that a minimal prime ideal of $\bar{\mathfrak{p}}_1+(\bar{a}_{j+1})$ must either be $\bar{\mathfrak{p}}_1$ itself or its rank will exceed that of $\bar{\mathfrak{p}}_1$ by unity. Since we can arrange that $\bar{\mathfrak{p}}_1$ and $(\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_j)$ have the same rank, the inequality

$$\operatorname{rank}(\bar{a}_1,\bar{a}_2,\ldots,\bar{a}_j,\bar{a}_{j+1}) \leqslant 1+\operatorname{rank}(\bar{a}_1,\bar{a}_2,\ldots,\bar{a}_j)$$

follows. We now see that, because rank $(\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_s) = s$, we must have rank $(\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_j) = j$ for each j; accordingly, by a well-known theorem,

$(\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_j)$ is *unmixed*: that is to say that *all* the prime ideals of $(\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_j)$ have rank j. Since $(\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_j)$ is unmixed and of rank j and since $(\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_j, \bar{a}_{j+1})$ is of rank $j+1$, we have

$$(\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_j) : (\bar{a}_{j+1}) = (\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_j) \quad (j < s). \tag{F}$$

Note that (F) holds, with the natural conventions, in the extreme case when $j = 0$. It now follows from (F), by successive applications of Theorem 9, that $\overline{(a_1, a_2, \ldots, a_j)} = (\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_j)$

for $1 \leqslant j \leqslant s$. Let us compute $\chi[r, (\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_j)]$; $\chi[r, (0)]$ is, from the definitions, the number of power products of $X_0, X_1, \ldots, X_n$ of degree r: that is to say it is the coefficient of x^r in $(1-x)^{-n-1} = (1-x)^{-m}$. But $(0) : (\bar{a}_1) = (0)$; consequently (by the note following Theorem 4) $\chi[r, (\bar{a}_1)]$ is the coefficient of x^r in $(1-x^{l_1})(1-x)^{-m}$. Again $(\bar{a}_1) : (\bar{a}_2) = (\bar{a}_1)$ and therefore by the same argument $\chi[r, (\bar{a}_1, \bar{a}_2)]$ is the coefficient of x^r in $(1-x^{l_1})(1-x^{l_2})(1-x)^{-m}$. Proceeding in this way we find that

$$\chi[r, (\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_j)] = \chi_m[r, (a_1, a_2, \ldots, a_j)]$$

is the coefficient of x^r in $(1-x^{l_1})(1-x^{l_2}) \ldots (1-x^{l_j})(1-x)^{-m}$. This proves the first assertion.

To complete the proof, we observe that (F) and Theorem 4 together show that

$$\chi[r, (\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_j, \bar{a}_{j+1})] = \chi[r, (\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_j)] - \chi[r - l_{j+1}, (\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_j)]$$

for all large r, whence, by the definition of the order of an ideal,

$$\operatorname{ord}(\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_j, \bar{a}_{j+1}) = l_{j+1} \operatorname{ord}(\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_j)$$

for $0 \leqslant j \leqslant s$. This gives

$$\operatorname{ord}_m(a_1, a_2, \ldots, a_s) = \operatorname{ord}(\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_s) = l_1 l_2 \ldots l_s \operatorname{ord}(0),$$

and, since $\chi[r, (0)] = \binom{n+r}{n}$, we also have $\operatorname{ord}(0) = 1$. This establishes the theorem.

REFERENCES

1. W. Krull, 'Dimensionstheorie in Stellenringen', *J. reine angew. Math.* 179 (1938), 204–26.
2. P. Samuel, *La notion de multiplicité en algèbre et en géometrie algébrique.* (Thesis) (Paris, 1951).
3. B. L. van der Waerden, 'Eine Verallgemeinerung des Bézoutschen Theorems', *Math. Ann.* 99 (1928), 497–541.

The Creation of the Universe

PROF. GEORGE GAMOW
Illustrated. 21s.

Advanced Dynamics

Two volumes
E. HOWARD SMART, M.A.
40s. each

Theoretical Aerodynamics

2nd Edition
PROF. L. M. MILNE THOMPSON, M.A., F.R.S.E.
40s.

A Treatise on Bessel Functions

and their Application to Physics
DR. R. C. GRAY and G. R. MATTHEWS
2nd Edition Prepared by
Prof. A. Gray and Prof. T. M. MacRobert
36s.

Macmillan and Co. Ltd.

HEFFER'S

BOOKS ON THE SCIENCES & HUMANITIES ENGLISH & FOREIGN

W. HEFFER & Sons, Ltd.
Petty Cury • Cambridge

THEORY AND APPLICATIONS OF DISTANCE GEOMETRY

By
LEONARD M. BLUMENTHAL
50*s. net*

This book presents a connected account of the development of abstract metrics, together with some applications to geometry, determinant theory, linear inequalities, and lattice theory. The aim of the book is to serve the dual purpose of a textbook in Distance Geometry for the graduate student, and a reference work for mathematicians interested in any of the many fields in which metric methods have proved useful.

OXFORD
UNIVERSITY PRESS